ACCESS CONTROL & SERVER SOFTWARE

User Manual

Version 5.3

Version Details

This document is applicable to the following software and firmware version.

Functionality	Version
IDU Access Control	5.4
IDU Server	5.4
IDU Firmware Upgrade Tool	5.4
IDU Firmware	5.2.0
Secugen Sensor Firmware	2.21
MS Windows 2000 Pro & Server	SP4
MS Windows XP	SP2
MS Windows 2003 Server	

This document is applicable to the following hardware.

Hardware	Version
IDU-5	IP65
USB Hamster	FDU02

Change History

The following changes have been made to this document.

Date	Person	Version	Change
16 May 2003	R. Boshoff	0.5	Initial Release
19 May 19 2003	M.C. Botha	0.6	• Updated form layouts from screen scrapes. • Added 'Options' and '3rd Party Applications'
22 May 19 2003	M.C. Botha	0.7	• Updated form layouts from screen scrapes.
2 May 19 2003	M.C. Botha	0.8	• Updated form layouts from screen scrapes. • Added reporting functionality.
12 June 19 2003	M.C. Botha	1.0	• Updated form layouts from screen scrapes. • Added options functionality • Added group allocation to multiple nodes functionality
Monday, July 07, 2003	M.C. Botha	1.1	• Updated Troubleshooting
Monday, July 22, 2003	M.C. Botha	2.0.25	• Updated form layouts from screen scrapes. • Firmware update. • Download DateTimeEvents from multiple nodes. • Transfer of persons and groups to unit includes an end date.
Monday, July 22, 2003	M.C. Botha	2.0.28	• Database password encryption added
Tuesday, September 02, 2003	M.C. Botha	2.0.51	• Updated form layouts from screen scrapes. • Updated functionality on IDU Setup form. • Fixed bug on networked enroll.
Thursday, September 11, 2003	M.C. Botha	2.0.61	• Updated form layouts from screen scrapes. • Added "PIN Required" to IDU Setup form.
Thursday, September 11, 2003	M.C. Botha	2.0.81	• Updated form layouts from screen scrapes. • Added "PIN Required" to IDU Setup form. • Enhanced Synchronize functionality • Enhanced IDU Setup functionality
Thursday, September 30, 2003	M.C. Botha	2.1.0	• Bug fixed: if invalid IP address is assigned to unit, all network settings is lost. • Bug fixed: synchronise functionality fixed on Person allocation form • Default for communications with device is set via popup menu on tree, no more prompts each time a unit is addressed. • Screens cleared up.
Wednesday, October 08, 2003	M.C. Botha	3.0.0	• Add: scheduling functionality • Add: database design update functionality • Change: user interface update • Bug: entering string delimiters (' or ") into fields causes update to fail.
Wednesday, February 18, 2004	E. Brink	4.0.0	• IDU-5 Optical: Add/Change property screen attributes
Monday, April 19, 2004	E. Brink	4.1.0	• Comprehensive update of document from previous IDU-3/4 versions, including: • USB Enrollment • RS485 communication • Various sensor & algorithm settings • Scheduling section BETA release
20 September 2004	T. Snyman		• Local enrollment
20 June 2005	E. Brink	5.0.0	• Comprehensive update of document due to new IDU-5 release, impacting the following areas:

			• Keypad functionality • Scanning of finger • Scheduling (bug fixes) • Export of date & time clocking events • Options Setup (Additional) • Enrollment • Limit of 2,048 fingerprint templates per IDU-5
14 February 2006	T. Snyman	5.0.1	• Replaced IDU5 pictures and back view with connections
01 July 2006	L. Badenhorst	5.3	• Support Desk details • Packaging changes • Installation application • Access Control Application • Node Cloning • Enrollment and Allocation (Maintain People) • Clockings and Search functions (Maintain People) • Scheduling simplified • Application Security (additional options) • IDU Log added (under Options) • Visitor Enrolment and Host Grant • IDU Server software update • Online Verification and Identification • Task Scheduler • IDU Firmware Upgrade Tool

TABLE OF CONTENTS

INTRODUCTION

1. BIOMETRICS OVERVIEW

(This section courtesy of Secugen Corporation)

Biometrics Overview

---

1. Why biometrics?

What qualities distinguish you from your neighbor? Of course our personalities differ to some extent, but there is a physical uniqueness as well. Once identified, these physical characteristics can be exactly measured, numbered, and counted. The statistical use of variations in these elements of living organisms is known collectively as biometrics. A person's biometric data can be collected and analyzed in a number of ways. This type of information is especially useful for personal identification, in which people are recognized by biometric-based security systems according to their own unique corporal or behavioral characteristics. Human traits and mannerisms that can be used in biometrics include fingerprints, voice, face, retina, iris, handwriting, and hand geometry.

Biometric methods of identification are currently being used to replace the less secure ID/Password method of user authentication, that is, verifying that people are who they say they are. Using biometric identifiers for personal authentication reduces or eliminates reliance on tokens we must carry with us, or the arcane strings of letters and numbers we are forced to memorize. Tokens, such as smart cards, magnetic stripe cards, and physical keys can be lost, stolen, or duplicated. Human memory is notoriously unreliable; according to recent estimates, at least 40% of all help desk calls are password or PIN-related. Losses attributed to fraud, identity theft, and cyber vandalism due to password reliance run well into the billions. Although passwords have traditionally been used for personal authentication, they have nothing to do with a person's actual identity!

Biometrics can be integrated into any application that requires security, access control, and identification or verification of people. With biometric security, we can dispense with the key, the password, the PIN code; the access-enabler is you - not something you know, or something you have in your possession. Remember, biometrically secured resources are based on who a person is, effectively eliminating risks associated with less advanced technologies, while at the same time offering a higher level of security and convenience.

2. Biometrics Applied

Biometrics security technology basically acts as a front end to a system that requires precise identification before it can be accessed or used. That system could be a sliding door with electronic locking mechanisms, an operating system, or an application where individual users have their own rights and permissions. In computer security, the term biometrics refers to authentication techniques that automatically check measurable biological characteristics of end users.

Examples include computer analysis of fingerprint minutiae data or speech patterns. Of course, this is partly what passwords have done all along. Again, the problem is that a password has nothing to do with your actual identity. There is simply no foolproof way to make password-protected systems completely safe from unauthorized intrusion. Nor is there any way for password-based systems to determine user

identity beyond doubt.

3. Typical Biometric Systems

- Fingerprint Recognition
- Face Recognition
- Iris Recognition
- Hand Geometry
- Voice Recognition
- Signature Recognition

Comparison
Popular biometric systems in use today include iris recognition, voice recognition, and fingerprint recognition systems. Iris recognition is extremely accurate but expensive to implement, and scanning the human eye is a sensitive issue that many find alarming. A typical voice recognition system is much less expensive but often exhibits unacceptably high FRR stemming from illness, hoarseness, or other throat problems. Fingerprint recognition is generally considered the most practical choice for its reliability, non-intrusive interfaces, and cost-effectiveness.

4. Identification vs. Verification

There are two primary functions offered by any biometric system. One is identification, a one-to-many (1:M) matching process wherein a biometric sample is compared to a set of stored samples in a database. The other is verification, a one-to-one (1:1) matching process in which the biometric system compares an individual's biometric sample to previously enrolled data for that user. The process of verification narrows the biometric database search by including other identifiers such as names or IDs. The terms "verification" and "authentication" are sometimes used interchangeably because both terms are used primarily to establish a specific user's validity rather than to identify users by querying an entire database of biometric samples.

5. Authentication

Any systematic method of confirming the identity of an individual. Some methods are more secure than others. Simple authentication methods include user name and password, while more secure methods include token-based one-time passwords. The most secure authentication methods include layered "multimodal" biometric procedures. This is independent of authorization.

6. FAR and FRR

Most modern biometric security systems can be fine-tuned to fit the needs of either high security or low security environments. Increasing security in biometric systems sometimes makes them more finicky, resulting in an increased False Rejection Rate (FRR) - this is manifested when a registered user's biometric data (e.g. fingerprint minutiae data) is rejected by the system. In these cases, emphasis on ambient lighting, climate, or user training may be needed. The net effect of FRR is usually nothing more than inconvenience to users. However, if security is set too low, the False Acceptance Rate (FAR) may increase. This is potentially far more serious, since it involves an unauthorized person gaining access to protected resources. The FAR and FRR vary widely among different types and makes of biometric systems.

7. Expected Growth

The Internet has become a permanent fixture in the lives of millions worldwide. The range of transactions now performed online runs the gamut of our daily living, and the stores never close. From routine banking to booking hotel reservations, from Wall Street to your retirement fund, the modern business offers online services to stay competitive.

The ballooning growth in electronic transactions has resulted in greater demands for fast and accurate

user identification and authentication methods. Biometric technology is now being deployed as a means of tightening security and simplifying user access in a landscape once guarded only by expensive firewalls and easily cracked passwords, subject to configuration issues, human error, and malice.

Fingerprints are among the least intrusive and most reliable biometrics in use, generally considered the best choice for speed, accuracy, and cost-effectiveness. Advances in technology occur at a lightning pace, changing the way we do things at home and at work. Increasingly we find ourselves struggling to retain mastery of a host of constantly evolving technologies and services.

After years of research and development, biometric security systems are now in the forefront of modern security. Although public acceptance has lagged behind expectations for certain biometric applications, many concerns have been dispelled through persistent engagement and education, particularly in the area of fingerprint recognition.

The IDU ACCESS CONTROL SOFTWARE was specifically developed for use with the **IDU-5** device. The software can be installed on **Windows 2000**, **2003** and **XP** platforms, and can also be integrated with existing time and attendance systems.

2. PACKAGING & INSTALLATION

Packaging include the following:

- IDU-5 IP65 Optical Fingerprint Device
- CD with:
  - IDU Access Control Administration Software for Installation
  - IDU Server Software for Installation
  - IDU-5 User Manual (PDF)
  - IDU-Installation/Technical Guide (PDF)
  - IDU-5 Application Programming Interface (PDF)
  - USB device drivers
  - Acrobat reader
- Standard Serial Cable (RS232)
- 12V DC Power Supply (please note power supply is for South African conditions 220V convert to 12V)
- Side mounting screws (4) and washers for mounting the back plate.
- RJ9 and RJ12 connectors, with 100mm leads, for Wiegand and Relay outputs.

Power 6-12V DC – Pin connector feeding the device 6-12V DC

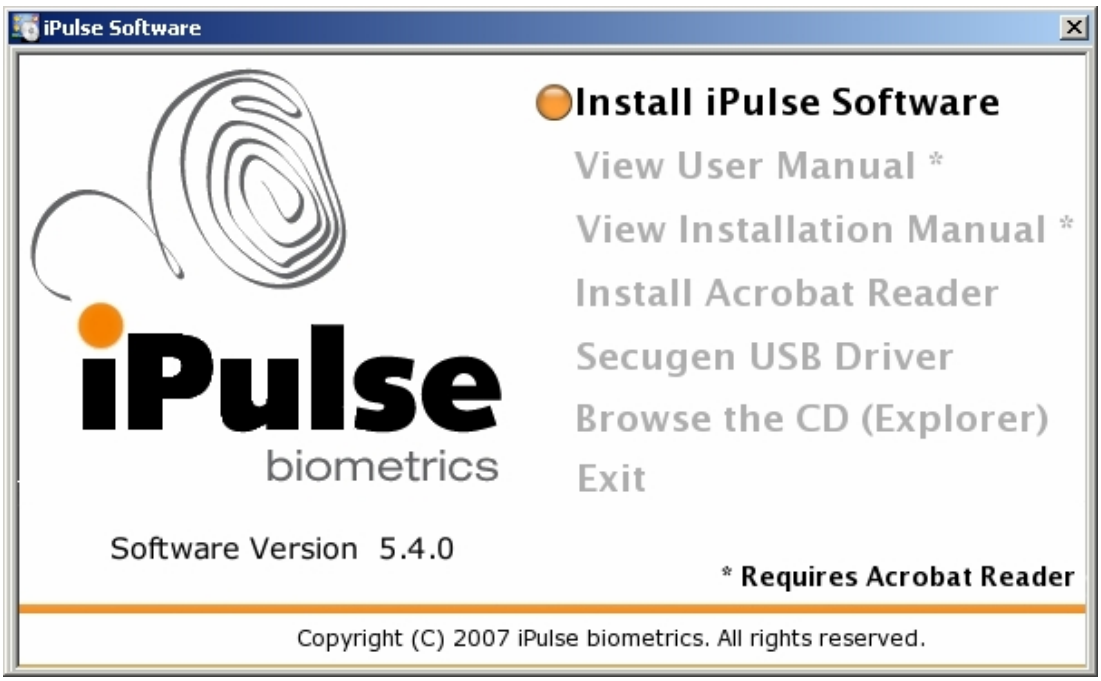
RS232/RS485 – RJ45 plug allowing for serial RS232 and/or RS485 communication, please refer to "Installation/Technical Guide" for pin layouts and detailed technical information
Signal Out – RJ9 plug , the IDU has two electronic outputs, please refer to "Installation/Technical Guide" for pin layouts and technical information.
Network – RJ45 plug, allows for Ethernet connectivity (10 Base/T). Each device has unique MAC address, implying no clashes with any other network peripherals.
Wiegand – RJ12 plug allows for Wiegand In & Out protocols. Generic interface allows for xx bit Wiegand interface (currently offering 26 and 44 bit).

For detailed technical information regarding this section, please refer to "Installation/Technical Guide"

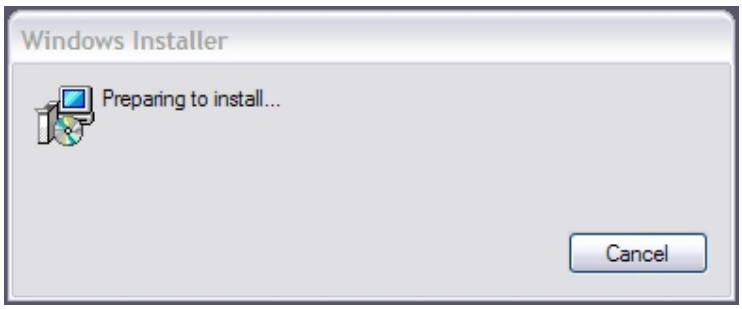
3. INSTALLING THE IDU ACCESS CONTROL SOFTWARE

Insert the latest CD into your CD ROM drive. Setup should start automatically, as the CD contains an Auto-run feature (else run "IDUSetup.exe"). Make sure you uninstall a previous version prior to installing the new software. This can be done under Add or Remove Programs under Control Panel.

The software has been tested on the following Microsoft Operating Systems:
Windows 2000 Pro and Server SP4
Windows XP
Windows 2003 Server

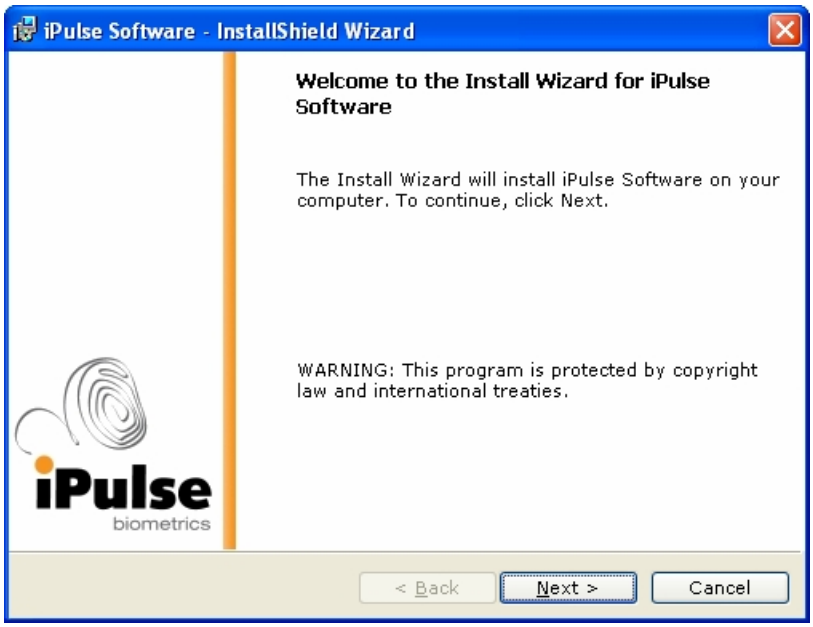


Select "Install iPulse Software" to start the installation, and the "Windows Installer" screen should appear.



If you do not have the latest Jet 4.0 OLE and MDAC versions installed on your PC, setup will automatically start the installation of these drivers and restart your PC. In this case you have to restart the installation procedure as described above.

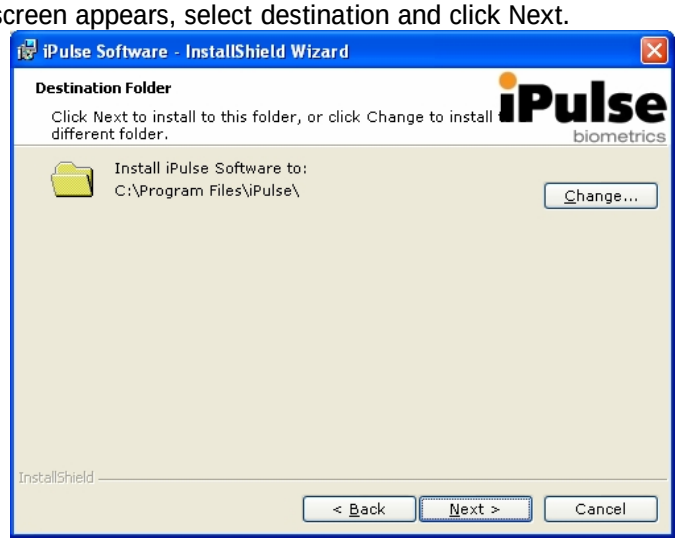
The InstallShield wizard screen appears, soon followed by the Welcome to InstallShield screen, click Next.



The License Agreement screen appears. Read the User License Agreement, and if you agree to it, tick I accept and click Next.

The Customer Information screen appears, fill it in and click Next.

The Destination Folder screen appears, select destination and click Next.



The Setup Type screen appears, select appropriate type and click Next.

Typical: Access Control Application
Server Application
Firmware Upgrade Tool
IDU and Sensor Firmware
Documentation

Minimal: Access Control Application

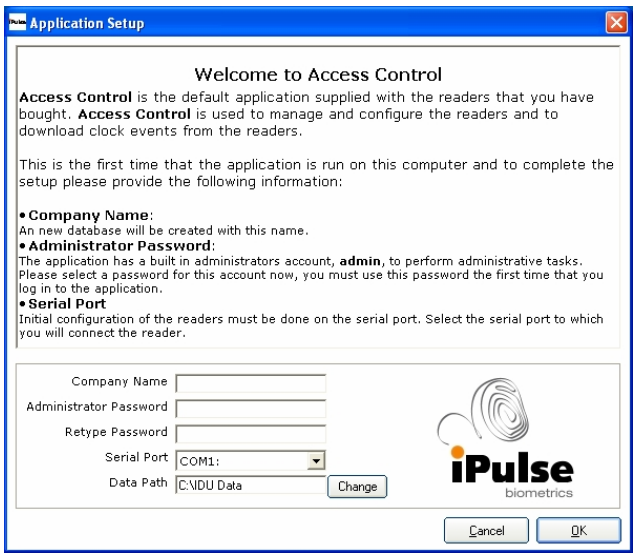
Custom: Same as typical, but selectable (recommended for advanced users)

Click Next, and Install.

The Install Wizard Complete screen appears, deselect Launch the program, and restart your pc.

4. STARTING (LOGIN)

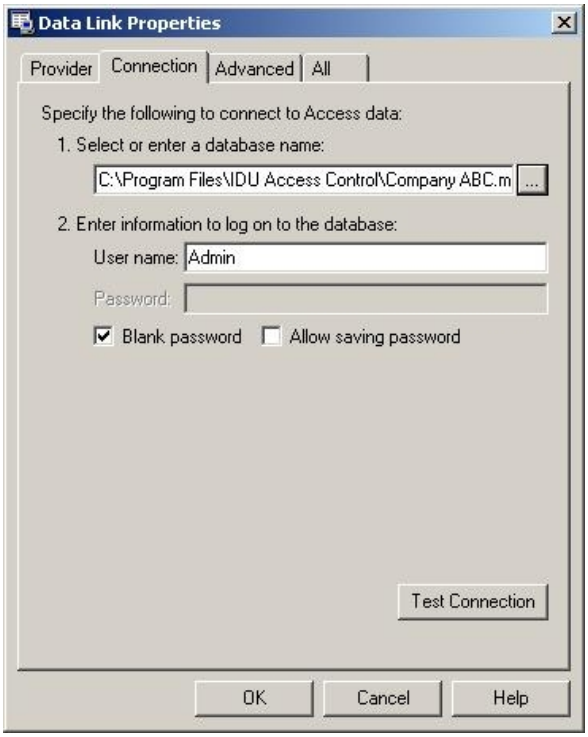
The very first time the application starts up the “Application Setup” screen is displayed.



The above screen only appears the 1st time the application is started – after the relevant detail has been entered the application will automatically create a database. The previous version of the application the user had to manually point & select a database – this new enhancement has been introduced to eliminate that problem. However the next time the application is started it will allow for manual change & pointing to user selected database – as per “Login Screen” below. After all detail has been entered please click “OK” button – the previous screen will only appear on 1st time installations.

The “Login” screen is displayed at activation of the application – please enter the relevant user name & password to enter the application.

If the ‘Select Database’ Checkbox is checked, select ‘Microsoft JET 4.0 OLE DB Provider’ which is the default option. On the second tab, click the select button (‘…’) and on the ‘Open Dialog’ point to the Access MDB file (standard license free database supplied with the application) to be used.



If login & database connection is successful, the IDU Menu will be displayed. Please note the previous section regarding the selection of the database is only done the first time the application is installed & executed, reason being the software is database independent, implying the windows software can run on any OLEBD database. (simply point to the respective OLEDB driver and database). This allows for flexibility should the requirement be to utilize e.g. Oracle, SQL*Server, Sybase, Informix, etc. as a database. The Access (MDB) database distributed with the application is license free, using Microsoft ADO Jet database access driver.

5. IDU ACCESS CONTROL BASICS

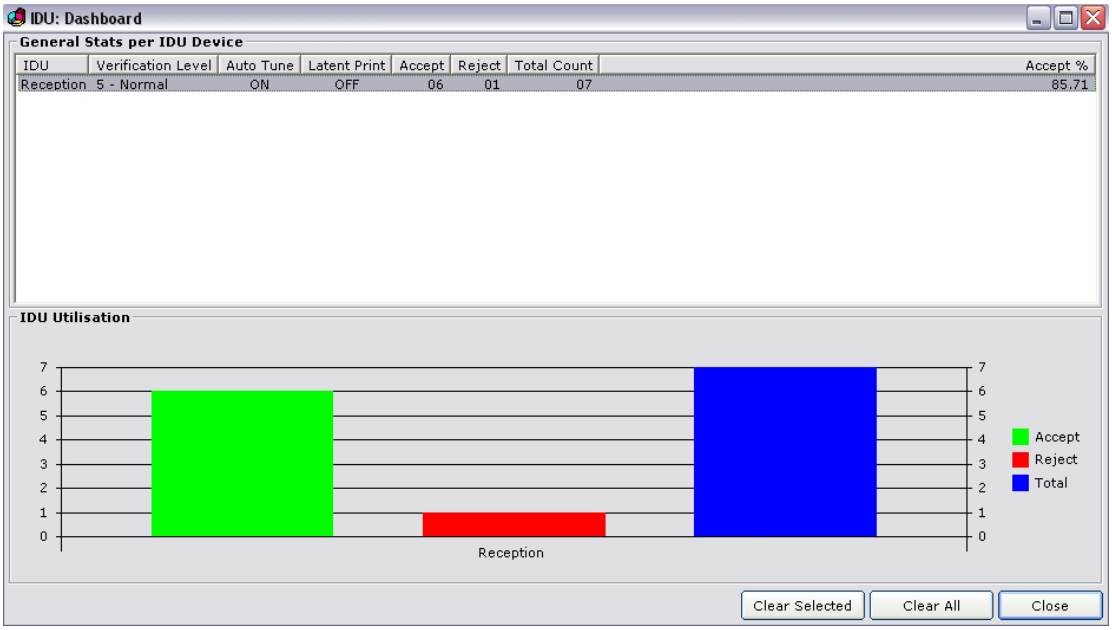
Button Caption	Functionality Available
Dashboard	Display graphical information pertaining to the number of successful and unsuccessful recognition events per IDU unit – this gives an indication (per unit) of the utilization and possible risk areas for failed identified fingerprints – also this provides feedback per device per security setting.
Access Control	Allows for a generic setup, control and configuration of multiples IDU devices – this area include the following functionalities: - generic setup of access control tree as per organizational requirement; - configuration (properties) per IDU devices e.g. separate security levels, naming of devices, network settings, relay delays, LCD display, time settings, etc.; - upgrading of IDU firmware; - Allocation of people to specific IDU devices (also per group or department); - Specifying IDU devices as access control, opening door or simply clocking station for time & attendance purposes; - Downloading of clocking events from specific IDU devices; - Specifying communication protocols e.g. RS485, RS232, Ethernet (network), etc. - Testing communications - Cloning of IDU devices - Opening of relays
Export Clocking Events	Export date time events as captured by the IDU unit(s). This allows for date parameters to export to a standard csv file, to be saved, edited and imported into time & attendance or payroll/wages applications. Mentioned report depicts persons per device e.g. Store room entrance and also displays the date and time of entry and/or exit.

Maintain People	Manages your central database of enrolled people, this section allows for the following: - enrollment or take-on of new people New people has to be enrolled only once and from there can be allocated to various IDU devices; - each person's detail can be amended e.g. more than one fingerprint can be enrolled per person; - Enrollment can be done via IDU device over RS232/485 or network OR a separate USB enrollment station; - This section also makes provision for alpha numeric employee numbers, renumbering of people, allocation of people into groups or departments, etc.
Scheduling	Set access schedules/shifts for people
Application Security	Manage system security including adding/deleting users and changing their rights, login usernames & passwords.
Options	Set up system parameters
3rd Party Applications	Launches 3rd party applications from within the application
Reports	Generic Reports
Visitors	Visitor enrollment and host linking
About	Displays the Splash screen or about box
Exit	Shut down the application

5.1. Dashboard

Various statistics are kept on the performance of each IDU device, such as fingerprint acceptance, rejection and security settings.

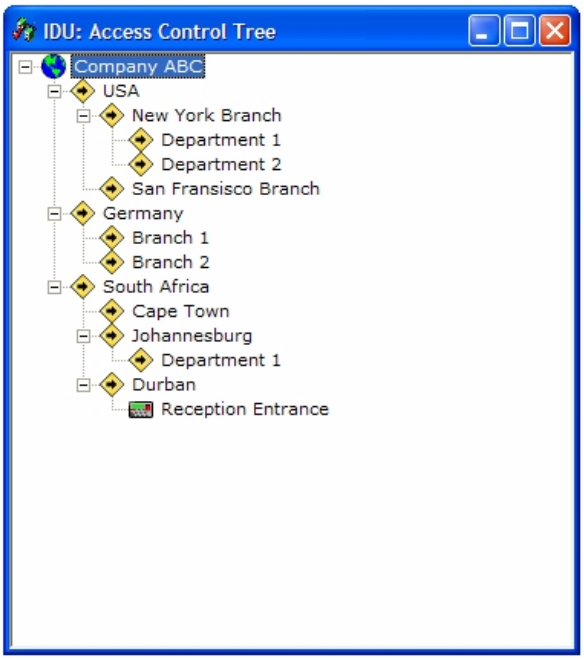
This indicates utilization per device and also identifies possible risk areas e.g. too much rejections in certain areas. Also this could aid in security level settings e.g. too much rejections could indicate too high a false rejection rate, implying identification security level perhaps too high for specific device. (refer to Glossary of Terms: False Acceptance versus False Rejection Ratios) The "Clear" buttons allows for resetting or clearing statistics.



5.2. IDU: Access Control Tree (Administration & Navigation)

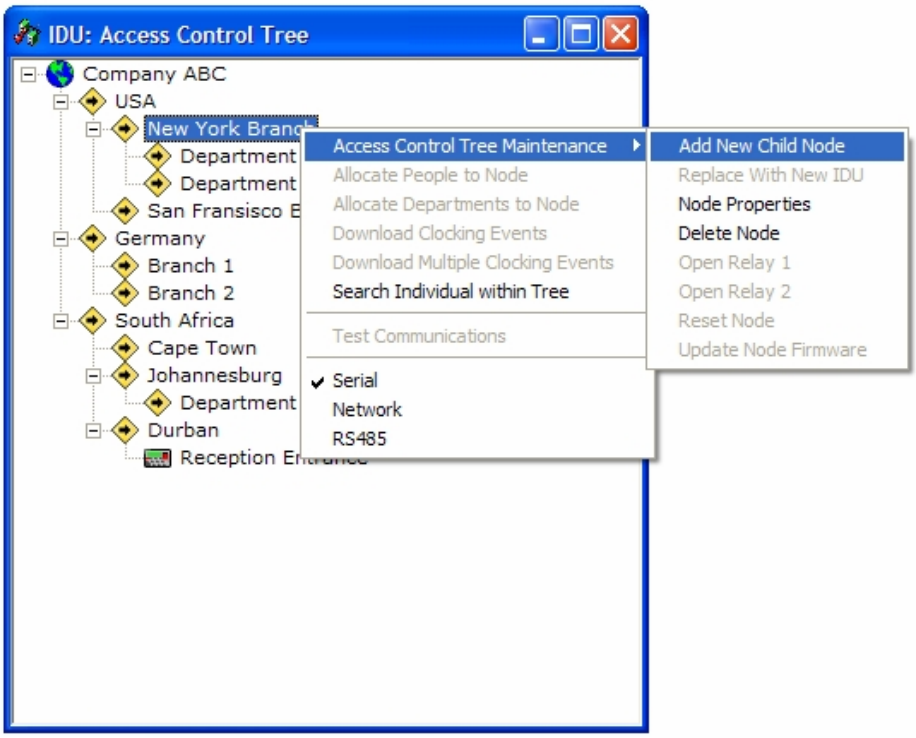
This option is the main user interface: (right click per node to display pop-up/context menu for applicable functional areas)

Note this section only deal with the basics of the “Access Control Tree” i.e. adding, deleting, renaming, etc. The rest of the functions on the pop-up/context menu will be addressed separately within this document. This section familiarizes the user with the tree and the navigational aspects thereof.

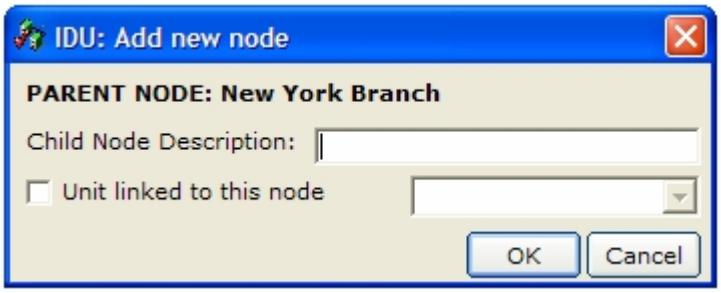


Generic setup of the "Access Control Tree": Initially when installed for the first time the tree has only one entry or node, namely the root – the root entry's name can be changed to suit your company. (Node Properties) By right clicking on the node a pop-up/context menu will appear, allowing for child nodes to be added – each and every organization can configure their own custom tree to meet their requirement. This tree could typically depict the physical hierarchical layout of your company – note that each functional area on mentioned pop-up/context menu will be discussed separately. The only limitation regarding the amount of nodes in the tree is 65,000 – otherwise you may add as many nodes, sub or child nodes as per requirement.

Add new child node: Right click on the "parent" node under which you would like to add a child, the following window will appear:

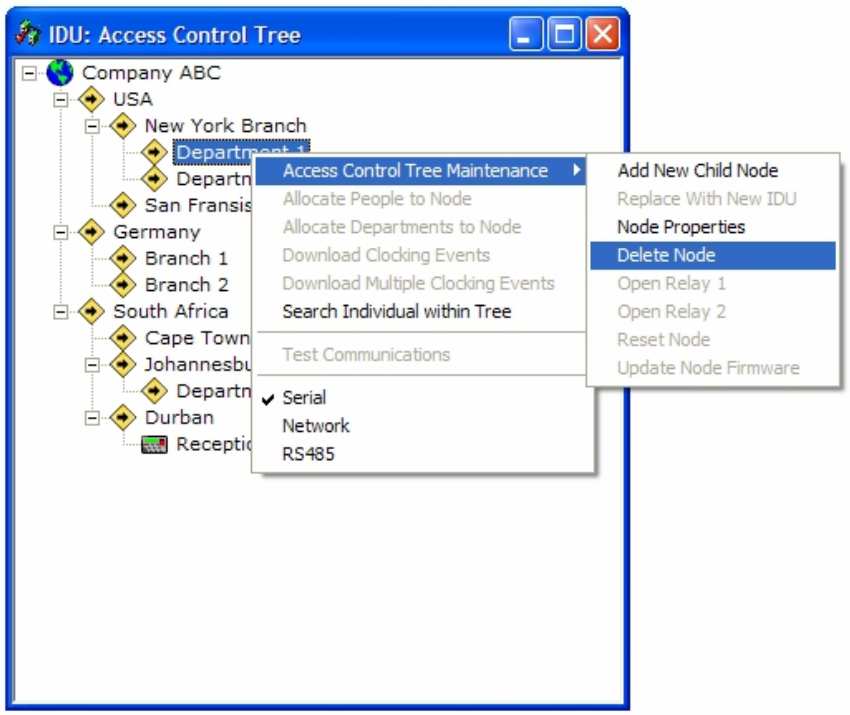


By clicking on the "Add new child node" option the following window will appear – please note that I want to add a new child node under the "New York" branch.

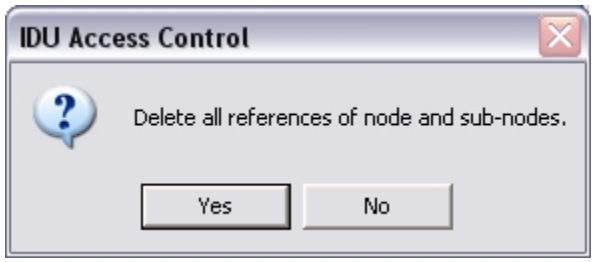


Please enter your new node description/name in the description field e.g. Financial Department and press the OK button. (for now let's leave the other fields available on the window – we will deal with this later when linking an actual IDU device to the node) By pressing OK the node would have been added to your tree, under the "New York" branch. You may go as wide and as deep in tree as might be required.

Deleting node: Right click on the node which needs to be removed from the tree and look for "Delete Node" option on the pop-up menu.



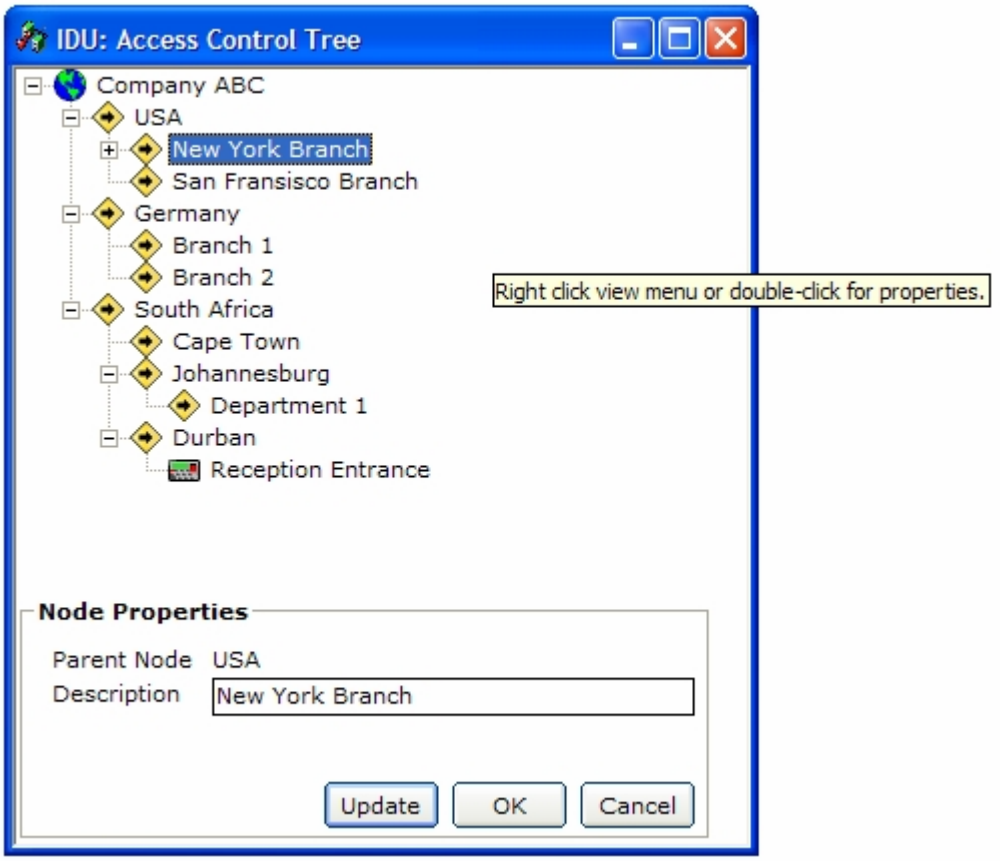
By selecting the delete option you will be prompted with the following window:



By selecting the "yes" option, the selected node for deletion will be removed – please note all sub or child nodes under deleted node will also be removed from the tree. By selecting the "no" option the deletion will be aborted.

Node Properties: Right click, on node which requires update, and navigate to the "Node Properties" option – by selecting the mentioned option the following window will appear, allowing for change of properties. **Note that one can also double-click on a node in the**

tree to access the node properties – double click always activates the property window of the node.

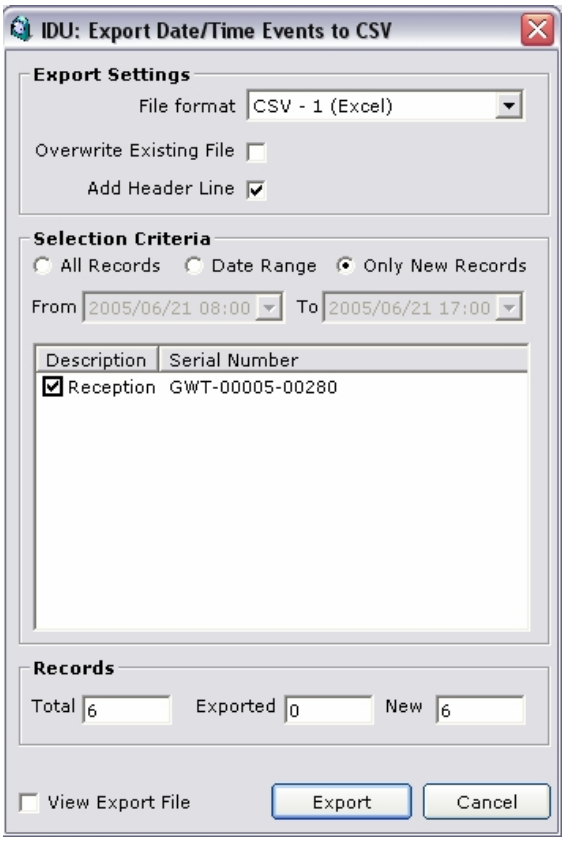


The node description may be changed now – please note that node properties, when an IDU device has been allocated against the node, changes quite dramatically and will be addressed further in this document.

5.3. Export Clocking Events

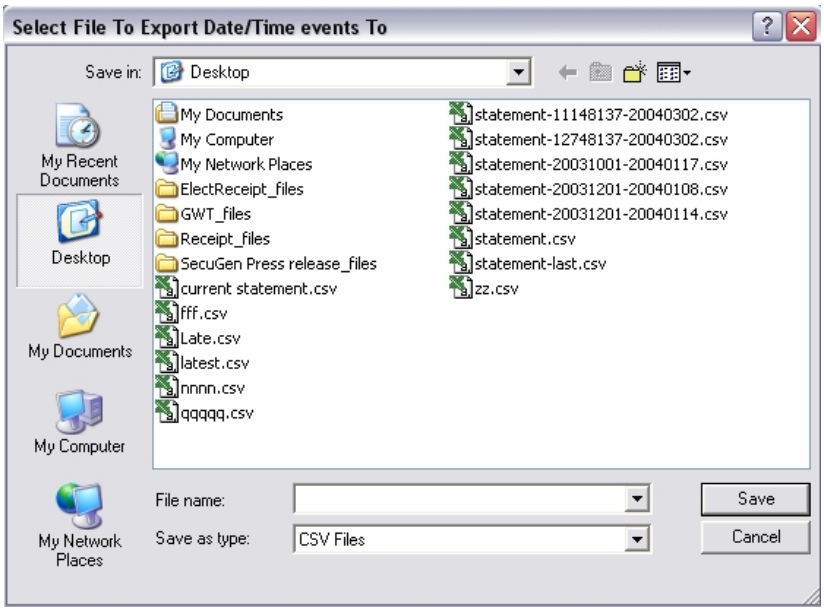
Date & Time events that have been downloaded from IDU devices can be exported to a 'csv' file – this allows for generic importing into Time & Attendance and/or Payroll or Wages applications.

Date parameters allow for only specific data to be exported, between dates as specified in parameter fields.



File format – Various formats for exporting clocking data exist, however all these formats is of the type CSV (comma delimited or separated values). This implies that external applications may import the clocking data – alternatively it may be saved and opened via Microsoft Excel for editing, etc.
Overwrite Existing File – If this box is checked it will imply that data to be exported will override previous data in export file.
Add Header Line - Adds a header line to the export file.
Selection Criteria – Various parameters exist for the selection of data, this is self explanatory.

By clicking the "Export" button, the following screen will appear, allowing for the saving of the exported data to a file name & destination of choice.



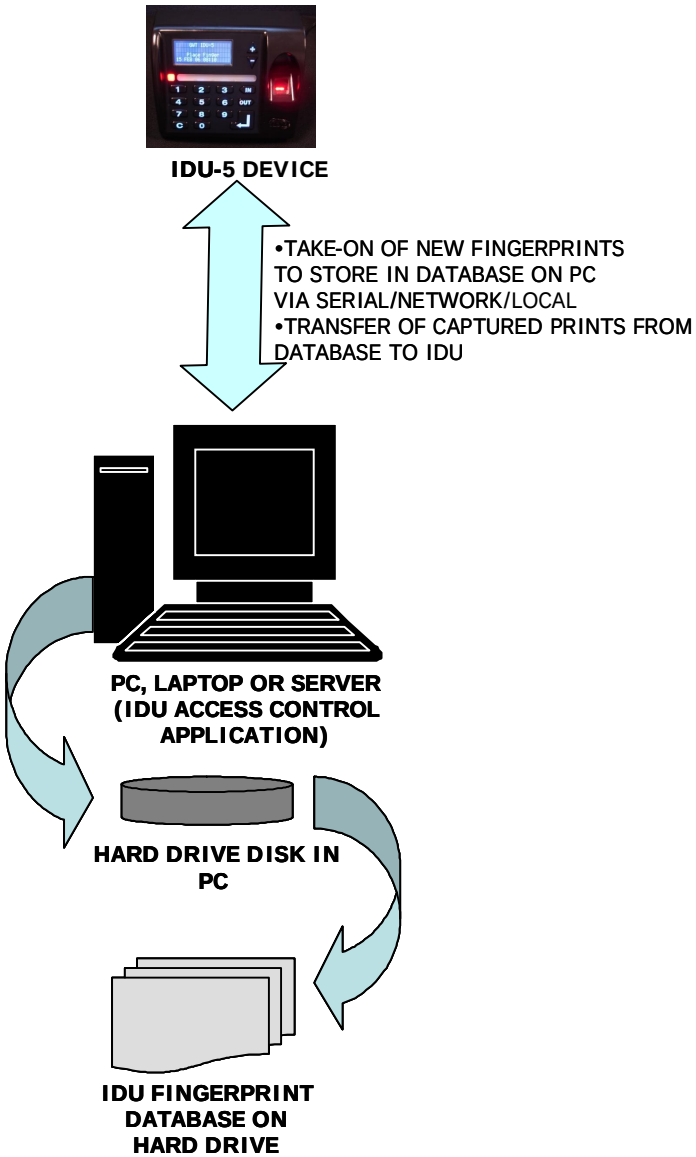
The exported file contains:

- Employee Number;
- Name & Surname;
- IDU device or Node clocked e.g. Reception Door; (as specified by the user in the Access Control Tree)
- Date & Time;
- In or Out Flag, indicating direction.

This data may be imported, edited, sorted, etc. (this is a standard Microsoft CSV file – by double clicking on it, it will be opened by Microsoft Excel)

5.4. Maintain People (Enrollment, Amendment & Deletion)

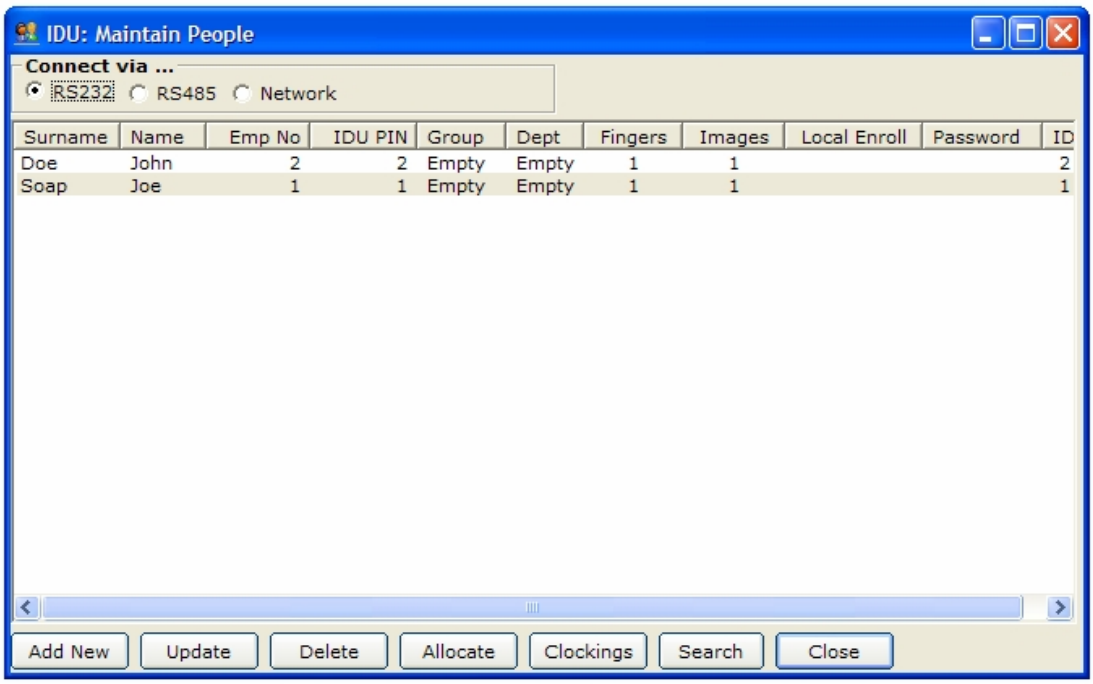
This option allows for people to be added, their respective detail/data to be changed and/or deleted from the central database. Please note that all data regarding person detail, including fingerprints always resides on the central database. Please refer to conceptual overview below for an understanding of the process.



The IDU-5 is used to capture fingerprint templates; during the direct capture process the fingerprints are stored on the PC, laptop or server's database and for the local capture process the fingerprints are captured directly on the IDU-5 device and then transferred to the database. A person needs to be captured only once and his/her data is available for all IDU-5 devices.

5.4.1. Add/Capture New Person

- This section describes enrolling or taking-on a new person on the IDU Access Control Database. There are 3 types of enrollment;
  - Direct: Fingerprints are captured directly in the database via a IDU-5 device that is connected on either RS232/485 or Ethernet (network).
  - Local: Person detail is captured directly in the database but the fingerprint minutiae is captured at a later stage on the IDU-5 device. After fingerprint minutiae are captured the database is then updated with this information.
  - Password: No fingerprint minutiae are captured and therefore no IDU-5 device is needed.



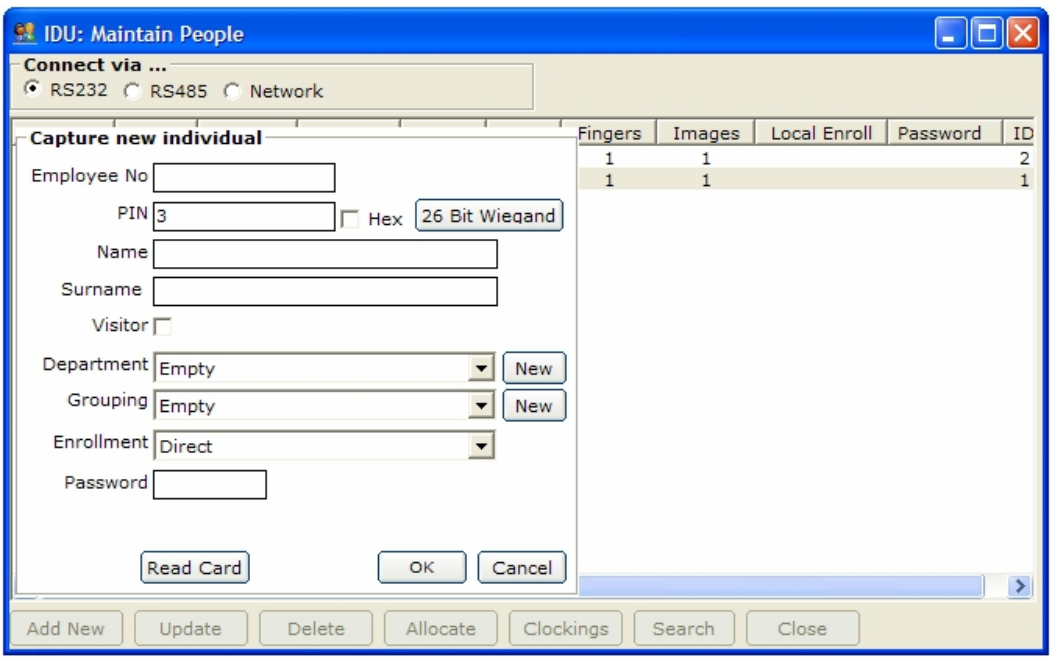
When selecting the “Maintain People” option from the main menu the above window will appear, allowing for all relevant maintenance to be done on already captured persons, including the capture of new individuals. Please note records may be sorted by clicking on the respective column headers.

Connect via ...: At the top of the window a selection has to be made via which protocol to capture the new individual, settings as follows:

- **RS232** (default): This connection type can only be done using the IDU-5 stand-alone unit via the serial cable. Should there be issues regarding communication please ensure the right communications port (serial) is selected as default in the "Options" function from the main menu – also ensure cable connection at both ends. (pc and IDU)
- **RS485**: This connection type can only be done using the IDU-5 stand-alone. Should there be issues regarding communication please ensure cable connection at both ends. (pc and IDU)
- **Network** (Ethernet): This connection type can only be done using the IDU-5 stand-alone unit via the network. Should there be issues regarding communication please ensure availability of network and the right network settings on IDU e.g. IP Address, etc.
- **USB:** This will only be available once a USB Hamster has been connected to the pc with drivers installed.

Depending on the communication selection a different enrollment/take-on screen or process might appear – the various enrollment options are discussed below

By clicking on the "Add" button the following window will appear.



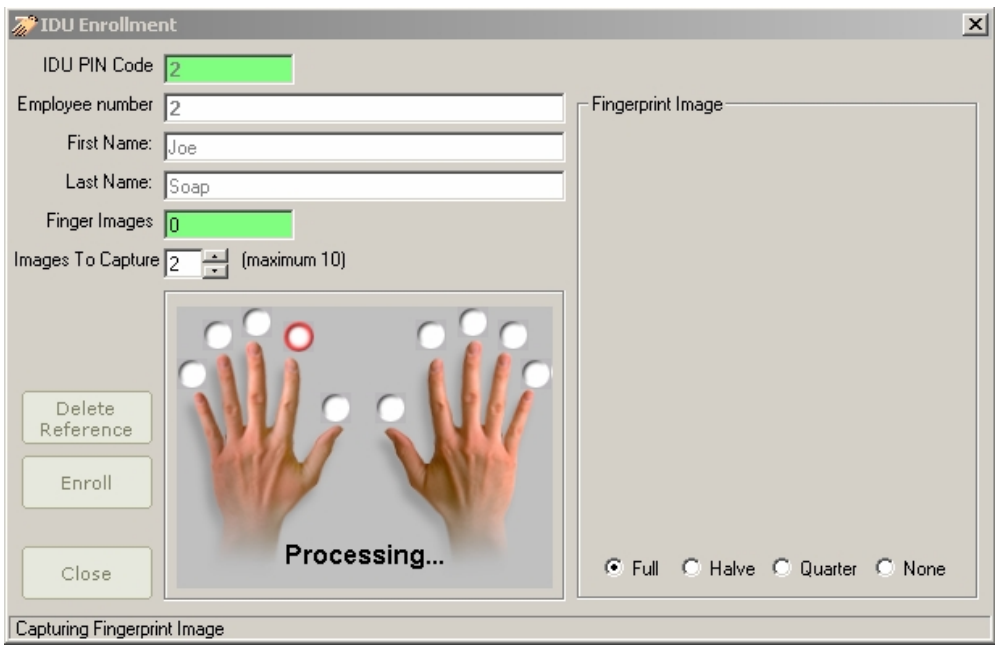
- **Employee Number** - Allows for an alphanumeric employee number. Please note that in the "Options" function a flag can be set to allow for unique employee numbers. The employee number will be utilized when exporting date & time events, for import purposes into Time & Attendance Applications/Payroll Systems. The export date & time events function is described in a different section in the document.
- **PIN** – Each and every new person captured automatically get allocated a unique PIN for verification purposes e.g. instead of identification a person can enter his/her PIN number on the IDU and verification will be done. (please refer to Identification versus Verification in glossary of terms).This could be used where certain people struggle with the identification of their finger(s) – give them an easy PIN and always ask them to enter PIN before scanning finger – this allows for:
  - o One-to-one verification;
  - o Dropping of security level which decreases false rejection rate and increases user convenience;
  - o Whilst still maintaining the same security as identification, due to one-to-one verification as opposed to one-to-many identification.
- **26 Bit Wiegand** – This button is used when the IDU unit (per person) needs to interface into Wiegand 26 bit. It will allow the user to enter a facility (site) code as well as the proximity card number. This will then serve the same purpose as the PIN, implying verification when the

person swipes his/her card. Please note for 44bit Wiegand (where no site code is required) the card number can be entered directly into the PIN field.

- **Hex** – This checkbox is used to display PINs in hexadecimal notation. Displaying PINs in hex is sometimes useful when working with very long PINs such as used in 44 Wiegand.
- **Name & Surname** – The applicable data to be entered here.
- **Department** – People may be allocated to groups or departments. Mentioned groups are generic of nature; implying new ones may be added as per requirement. This makes for easier transfer of people to and from IDU devices e.g. allocate group "Finances" to IDU called "Finance Door In". Allocation of people discussed separately in this document.
- **Grouping** - ???
- **Enrollment –** Select the enrollment type (Direct, Local or password). The default type (as selected on the "Options" screen) will be automatically selected.
- **Password** – This field has been included purely when a person's finger cannot be enrolled for whatever reason. Under normal circumstances this field must be left blank and only entered when no fingerprint for the person is to be enrolled. This will then still allow the person to clock or open door by first entering his/her PIN, then by breaking the infrared beam as if a finger has to be scanned – the IDU device will then prompt for the password. If both PIN and password match the clocking will be registered and the door opened.
- **Read Card** – This button is used when using proximity cards and the card number is unknown. If an IDU unit is connected to a serial port it can be used to read a proximity card and the value will then be entered into the PIN field.

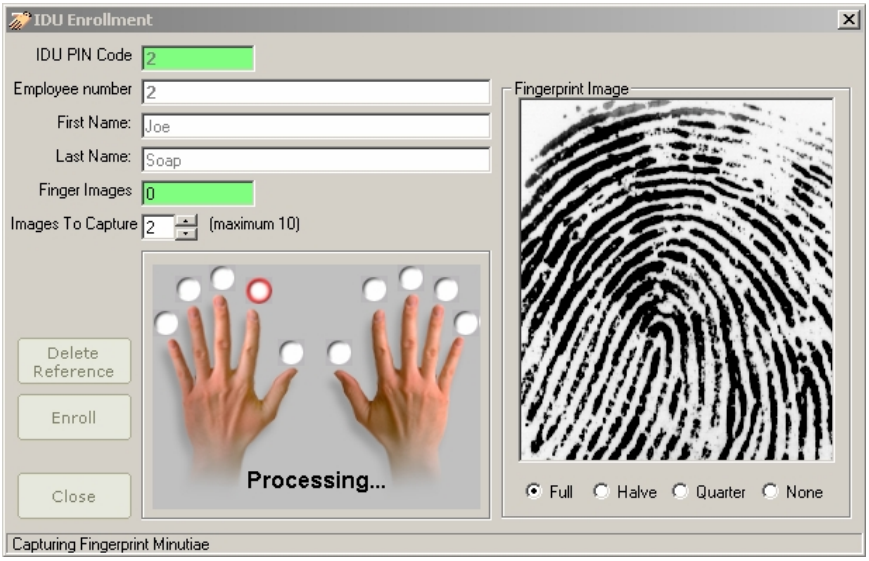
After completion of the above mentioned fields/data, the "OK" button must be clicked – the following window will appear, depending on the enrollment type selected. More than one finger per person may be registered – it is advisable to enroll at least two fingers per person – should one finger be damaged the person can still use the alternate finger

IDU-5 ENROLLMENT - DIRECT:



The above window's functionality is more or less the same for all the communications type except for the following differences:

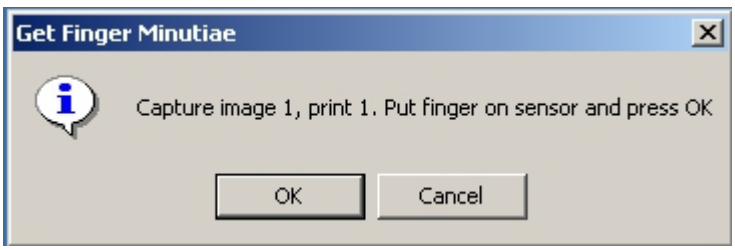
- Fingerprint image is only available via RS232 or RS485.
- The fingerprint image is displayed to the right side of the window – please note that a selection could be made to display full, halve, and quarter or none of the captured print. Seeing that a large amount of data must be transferred over serial the option has been given to select the size of picture to be viewed. The bigger the image size, the slower the data to transfer via the serial cable. Also note that when doing enrollment via the network the picture of the print is not available due to the size of the image to be transferred.



- When selecting the network/RS485 option to enroll new fingerprints a window will appear, showing all devices on. By selecting the device you wish to capture the new fingerprint the application will allow enrollment in the same manner as via RS232 (serial). Please note this is an extremely inconvenient manner of taking on new fingerprints.

The number of images to be captured per finger is selectable (each image of a finger consists of two prints) with a maximum of ten images per person.

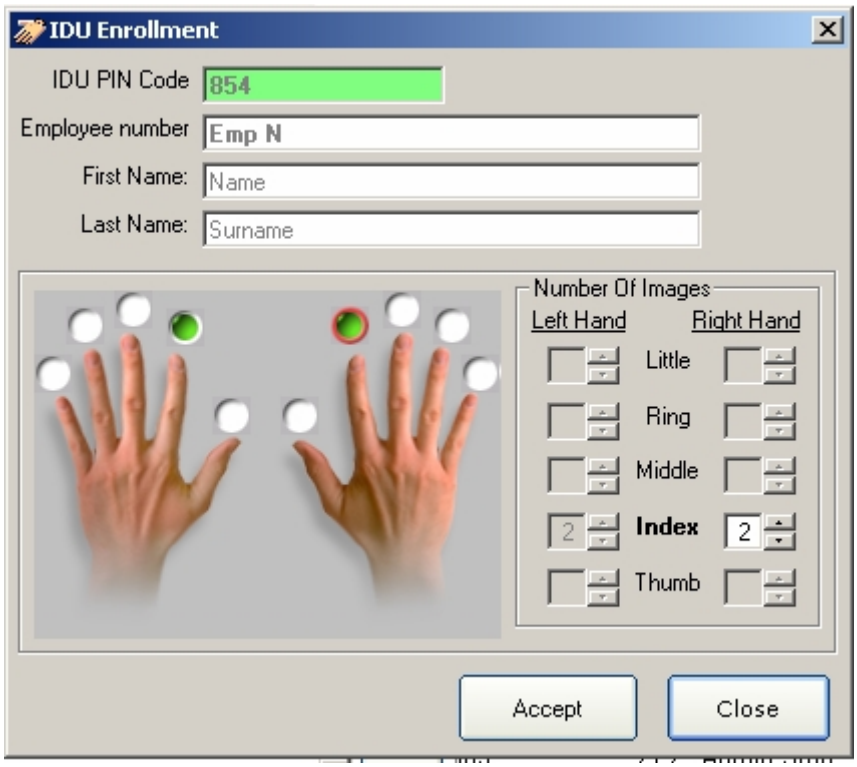
By selecting the finger to be enrolled and clicking enroll a window will appear. The IDU will scan the finger and present the image captured, as depicted above. Note that you will be asked to present the finger twice for each image to be captured. Two copies/prints of the fingerprint are always stored for identification purposes.



Throughout this process the user may at all times cancel to stop the process – applicable windows will guide the user, posing questions for abortion of the enrollment process. When aborted you may simply start again, until you get the required results.

The picture below shows the capture of the first print, using the “Full” picture option to be displayed – this will take longer than halve or quarter option due to the size increase of the picture to be transferred via the serial cable.

IDU-5 ENROLLMENT - LOCAL:



The fingers and the number of images to be captured per finger is selectable (each image of a finger consists of two prints) with a maximum of ten images per person.

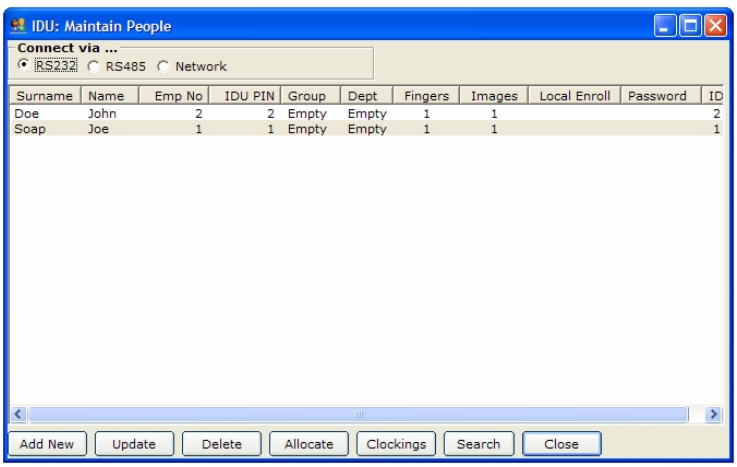
By clicking on a finger to be enrolled a selection box on the right of the screen will be available where the number of images to be captured can be entered. The data for images to be captured will be transferred (via the "Allocate People to Node" option in Access Control) to the IDU-5 device for the local enrollment process.

Once the data has been transferred to the IDU-5 device the following enrollment process is available on the device:

- Enter PIN and password for person to enroll on IDU-5 device.
- The device will prompt the user to put finger on sensor for Auto Tuning
- After the Auto Tuning the unit will prompt the person to put the applicable fingers/s on the unit for enrollment.

5.4.2. Update / Amend / Delete Person Data

By navigating the respective buttons as shown below, personal detail may be amended.



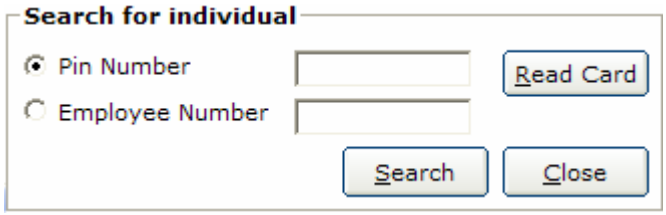
Update: To update a person's particulars, department, grouping and prints.

Delete: Remove a person completely from the IDU Access Control database. The system will not allow deletion if a person has been allocated to a node (IDU device) on the tree and the system cannot connect to the device to delete person – the person must 1st be removed from the respective node(s) manually. If the system can make connection via network it will automatically delete person from all IDU devices.

Allocate: To allocate or remove a person from an IDU device. Please note this option does not delete the person's record on the central database and the person could be allocated again to IDU or node(s). Make sure you select the correct communication method on the top of the page when allocating or removing people, as it will only connect to the relevant IDU/IDU's connected via this communications interface.

Clockings: Displays clocking events per person per IDU node. Note this data is also available from the export csv file option or the reports from the main menu.

Search: Search for individuals in the database by PIN or Employee number.



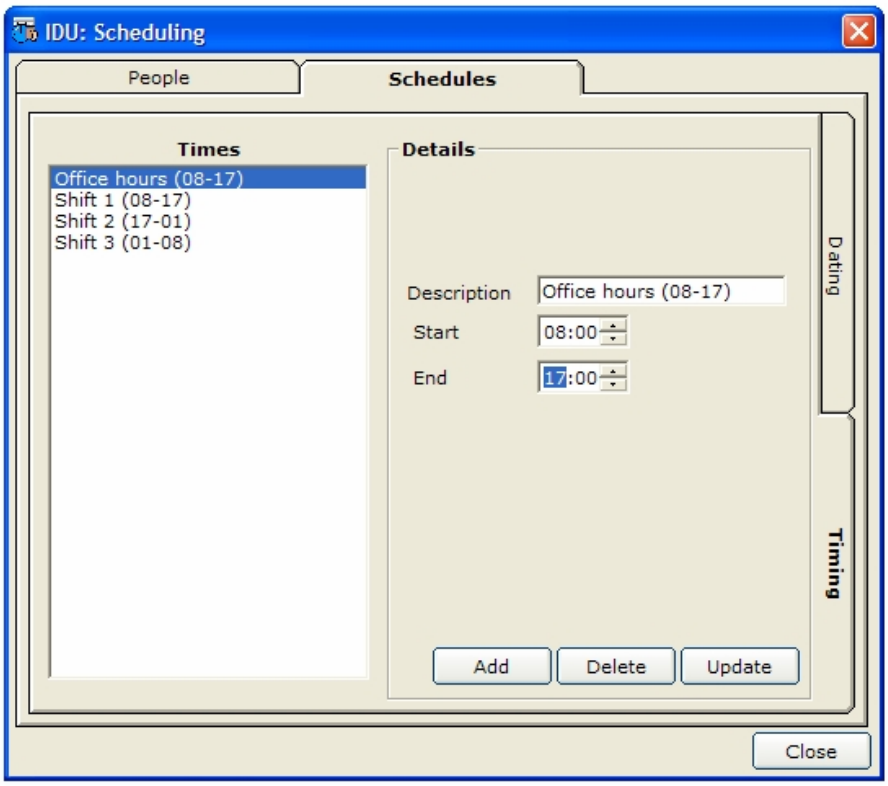
Close: Closes the Maintain People Window and returns to the IDU Menu.

5.5. Scheduling

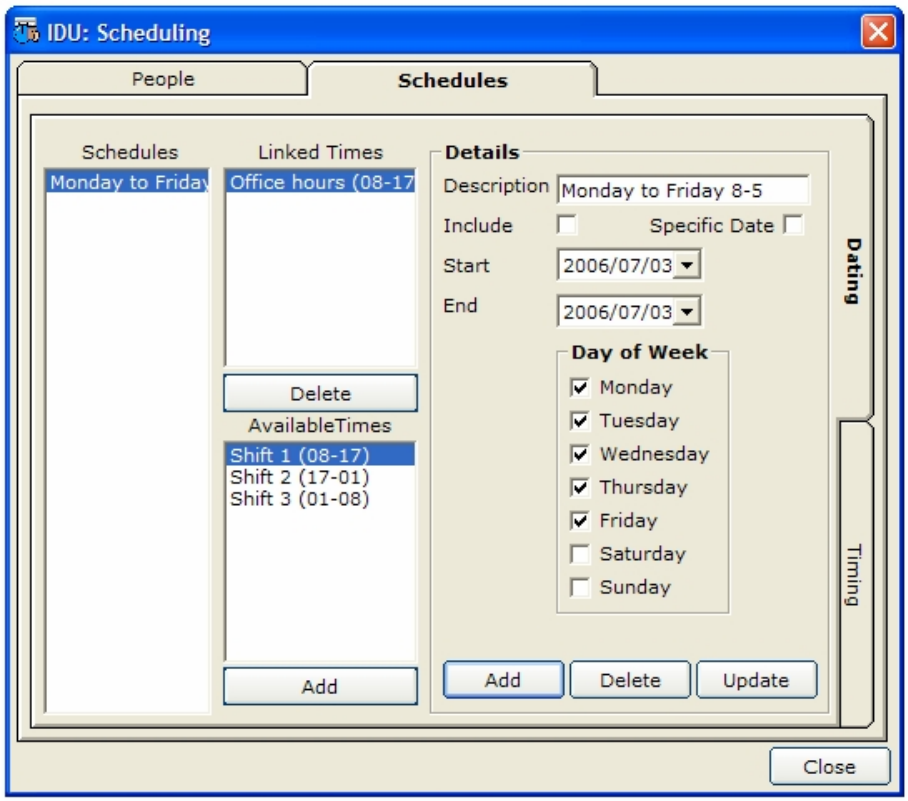
This feature is used for creating and assigning schedules to enrolled people, allowing them access to certain predefined readers at certain times of the day.

Schedules will NOT be available without the server application running on the pc, as the IDU will interrogate the server to verify whether access is permitted at that particular time (see 6.4 Allocation of People-Verify Schedule).

Timing – Create your shift here by typing a description, selecting start and end time and clicking on add. You can always modify the shift by highlighting it on the left of the screen, modifying it and clicking on update.



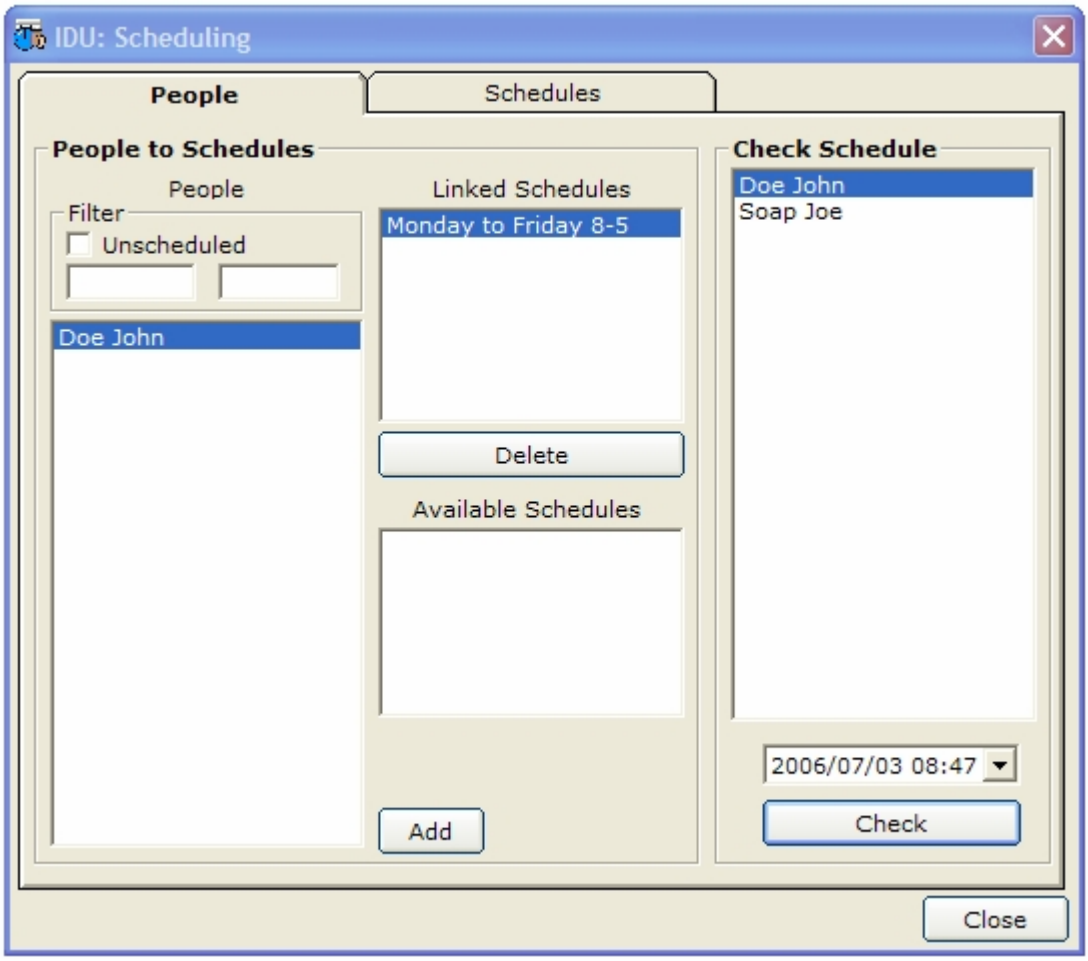
Dating – Here you link a shift to a schedule. Type a schedule description into the field provided, select Include (includes a specific date range only), or Specific Date (includes only a certain day), or tick appropriate day/days of the week. Click on the Add button, and the schedule is saved. You can also modify the schedule by selecting it under Schedules on the left, modifying it, and then selecting Update.



People – You assign schedules to people under this tab. Tick Unscheduled under Filter, highlight the person add the schedule to, Highlight the schedule under Available Schedule, and click Add. The schedule will now be linked to the person, and you can verify it by deselecting the Unscheduled tick box.

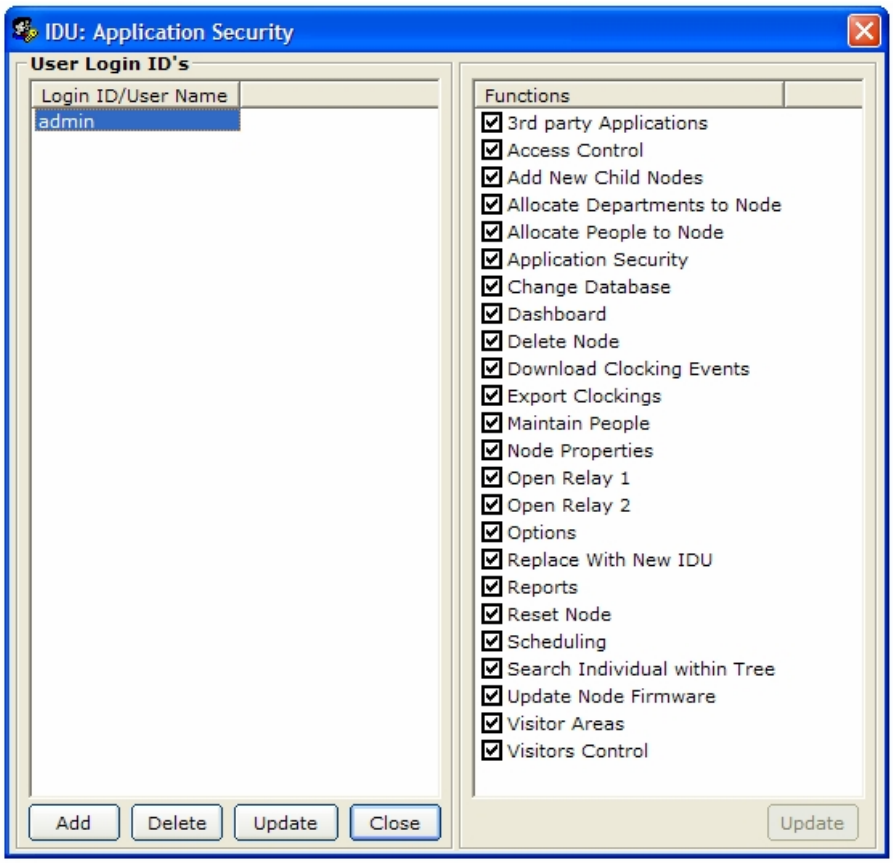
You can also check whether the schedule is working according to plan by changing the time and date under Check Schedule, selecting the person and clicking on Check. You will receive either Person Allowed or Person Not Allowed message, if the time selected is IN or OUT of predefined schedule.

You can remove a schedule from a person by selecting the person under People, selecting the schedule under Linked Schedules, and selecting Delete.

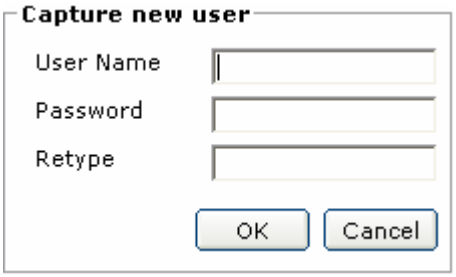


5.6. Application Security

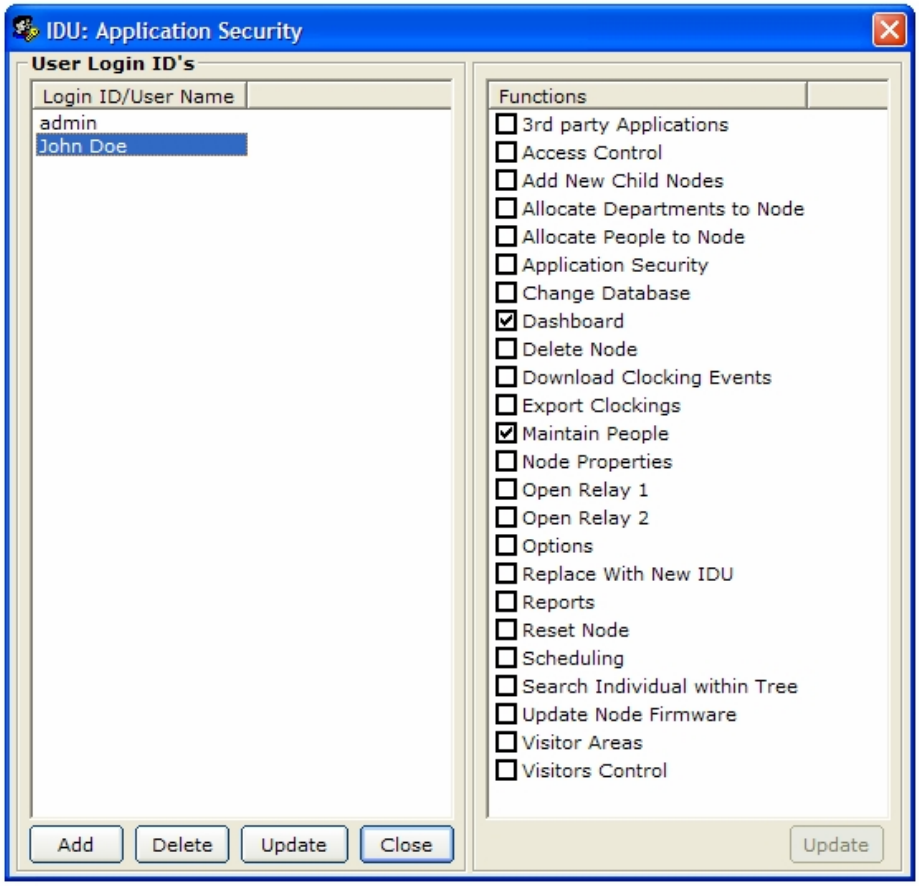
Multiple users for the IDU Access Control may be created, each with their own password and levels of accessibility to the IDU Access Control functions. The default user login and password is “admin” and “admin” respectively. It is advisable to change the admin password at the earliest convenience.



Add (User Login): This button allows for new users to be added to the system – the following window will appear. Enter the username and password – any alphanumeric string.



By clicking the OK button the user would have been added to the existing list of users that may log into the system – now allocate the relevant functions the person has access to.

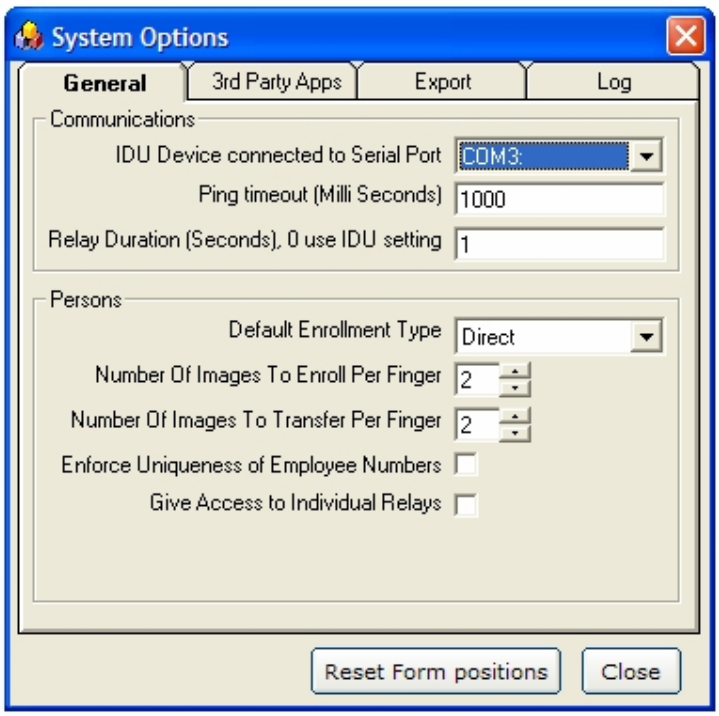


Functions are allocated by clicking on the checkboxes next to the function description – then click the "Update" button to effect the changes to the database. In the example above "John Doe" has been created with access only to the "Dashboard" and "Maintain People" functions in the IDU Access Control Application. As from now the new user may log into the system using their login user name & password.

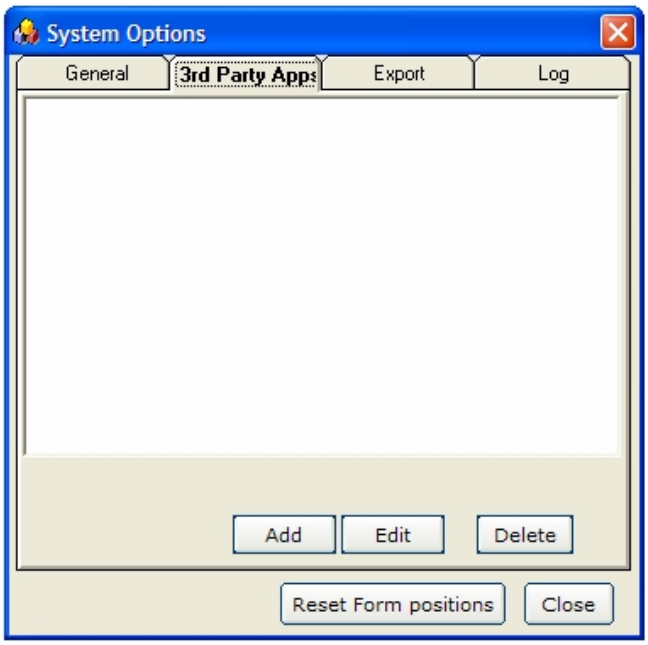
5.7. System Options & Setup of 3rd Party Applications

General Tab:

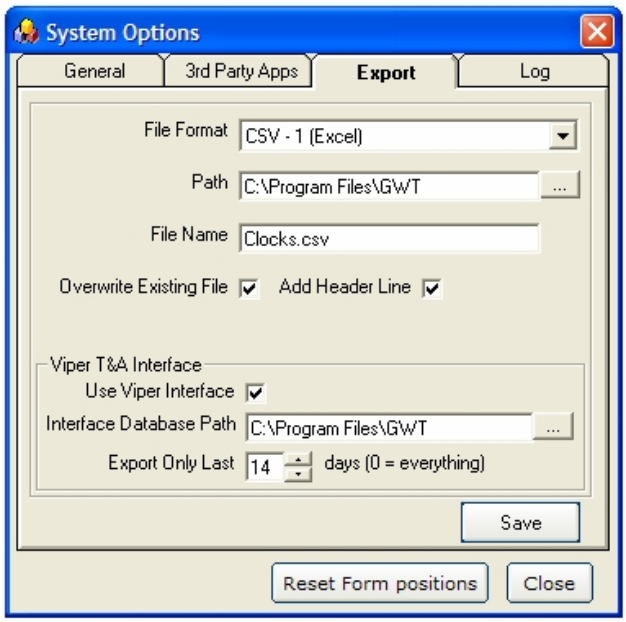
- **Communications:**
  - **Serial Port:** The serial port to be used when communication with IDU devices via serial (RS232/RS485). Typically when allocating an IDU device against a new node in the access control tree communication via RS232 (serial) needs to be established to get the IDU device's serial number and configuring it's network settings e.g. IP Address, etc. After which you can communicate with the IDU device via your network.
  - **Ping Timeout:** When accessing IDU devices over a network, this setting may be reduced for faster networks and increased for slower networks. This setting is only for the initial communication towards an IDU via a network
  - **Relay Duration:** Only applicable for network, when a relay is opened via the network.
- **Persons:**
  - **Default Enrollment Type:** The enrollment type to use when enrolling a new person (direct, local or password).
  - **Number Of Images To Enroll Per Finger:** Default number of images to enroll per finger when adding new persons.
  - **Number Of Images To Transfer Per Finger:** Default of number of images to transfer per finger when transferring persons to IDU-5 device. This number can be smaller than the number of images captured allowing the enrollment of multiple images per finger and then only transferring a subset of these.
  - **Enforcing Uniqueness of Employee Numbers:** Will enforce that each person must have an unique employee number.
  - **Give Access ...:** When this setting is checked, it will allow the user when transferring an individual to an IDU devices to specify certain relays to activated on a successful identification/verification.



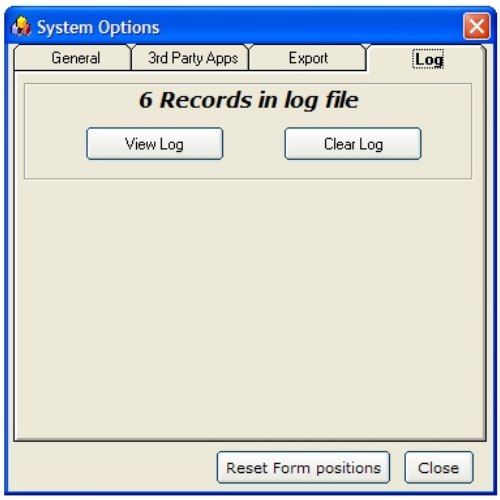
3rd Party Apps: This section allows for 3rd party applications (typically windows .exe programs) to be added to the system. Each 3rd party application will typically have it's own logic and purpose – a typical example would be after exporting date & time clockings, to automatically launch/run 3rd party application for integration into wages or time & attendance applications (default setting).



Export: This section allows for setting up the various export options. Note that this is self explanatory.

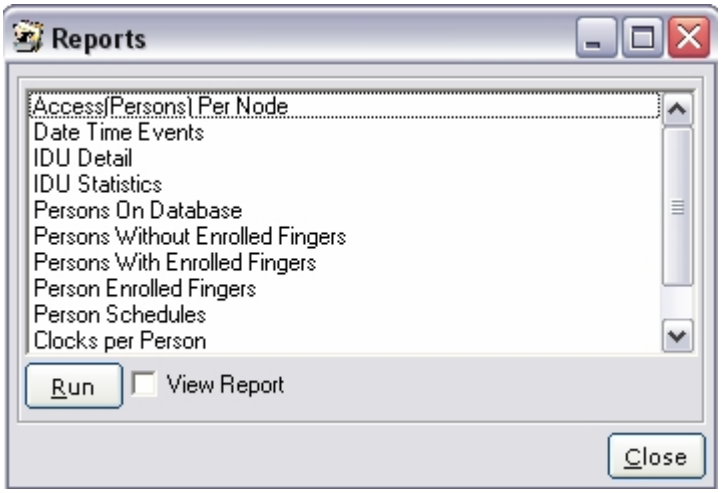


Log: This section logs all settings changed on an IDU unit.



5.8. Reports

This functionality provides basic/standard reporting capability. Reports are written to CSV format and the report could optionally be launch with the default application associated with this type of file.

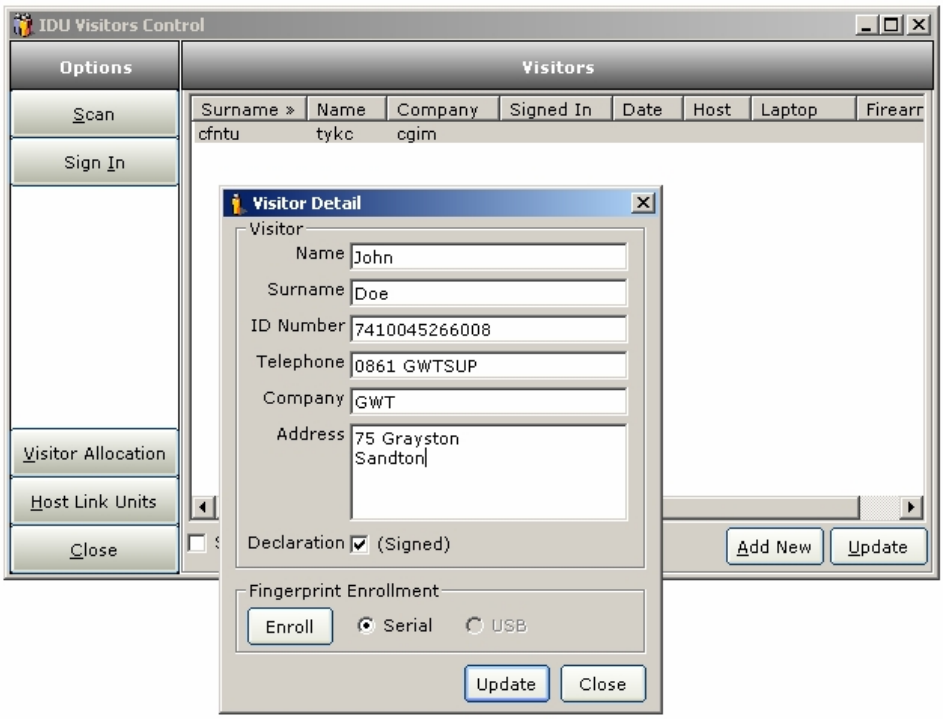


Reports can be viewed, edited and removed. Clicking on the **Load** button will add the standard reports to the database.

5.9. Visitors

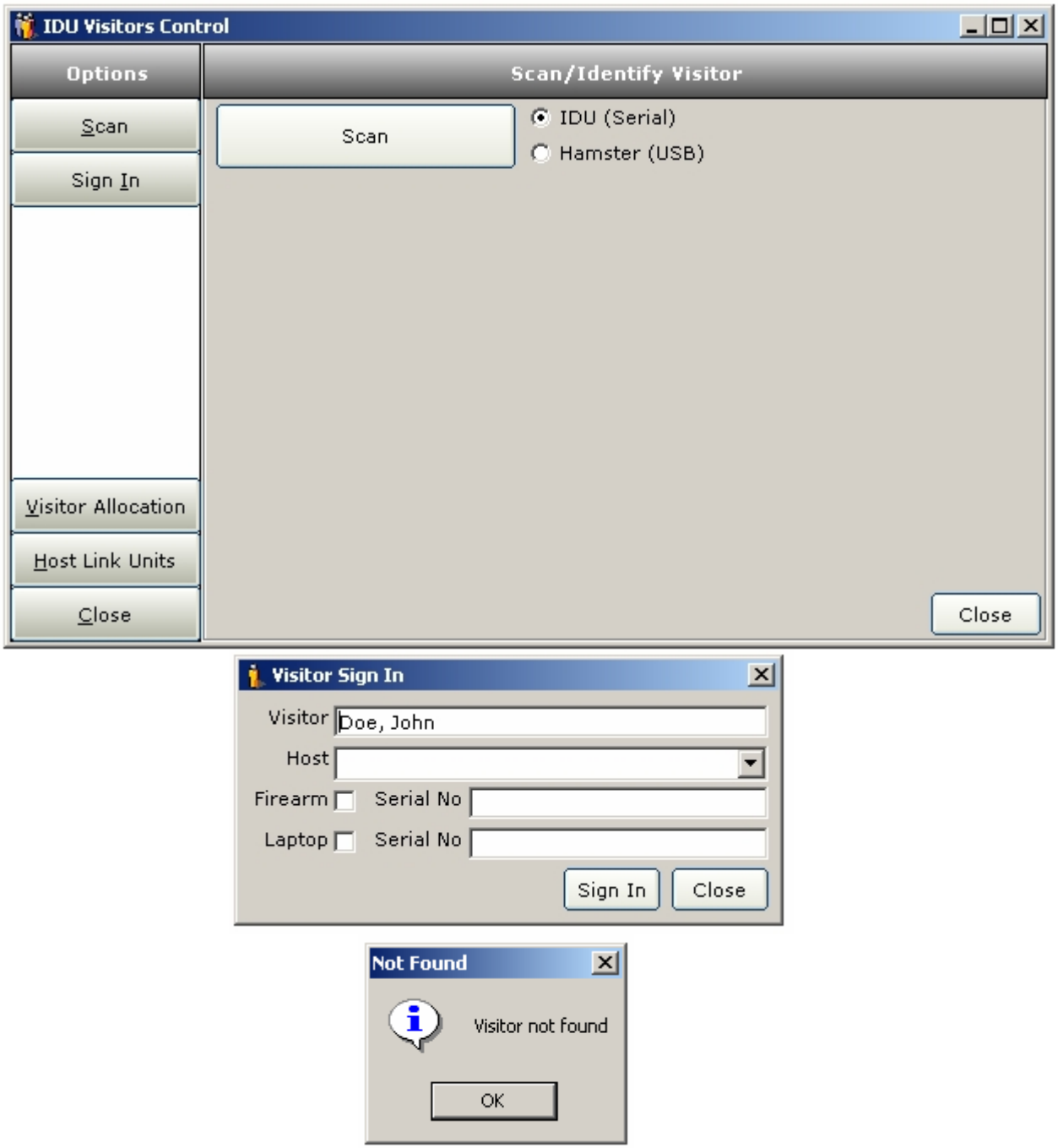
A basic Visitor Enrollment and Host Grant feature has been added in this software release, to ease the tedious job of managing visitors. You can now enroll visitors at your security reception area, and automatically allocate them to a predefined list of readers over the network.

Add New – You add new visitors by clicking on Add New, completing the Visitor Detail page, Ticking the Company Policy Declaration (if any), selecting the method of enrollment (Serial or USB), and clicking on Enroll. Follow the same procedure as in 5.4.1 - Local Enrollment.

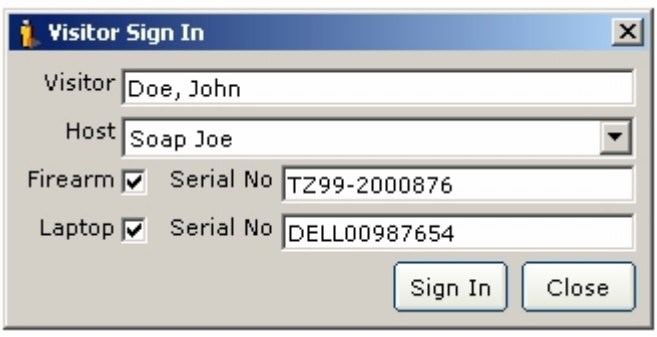


You can also update an existing visitor by selecting the visitor in the list, and clicking on Update.

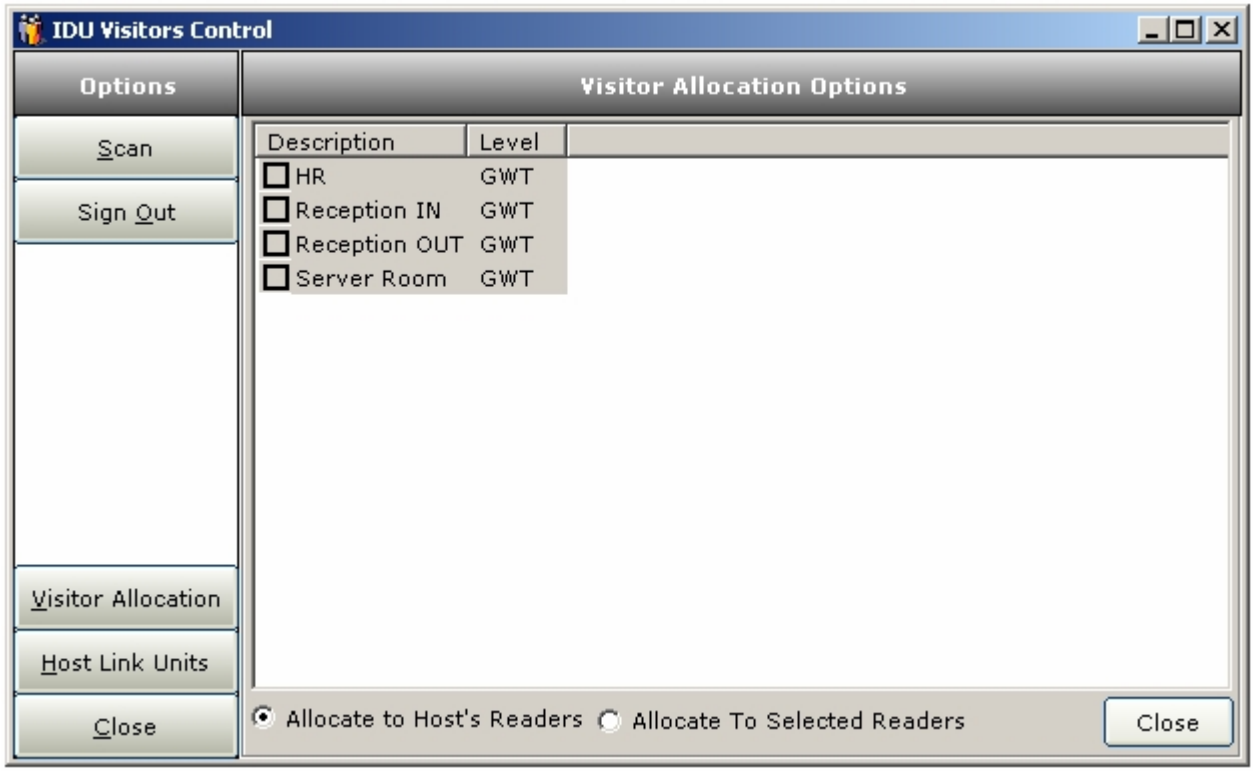
Scan – You can use this feature to search for a visitor already enrolled on the system. Select Scan, select serial or USB, and click on Scan. If the print is recognized, the Visitor Sign In screen will appear with the correct credentials, else the Not Found screen will appear.



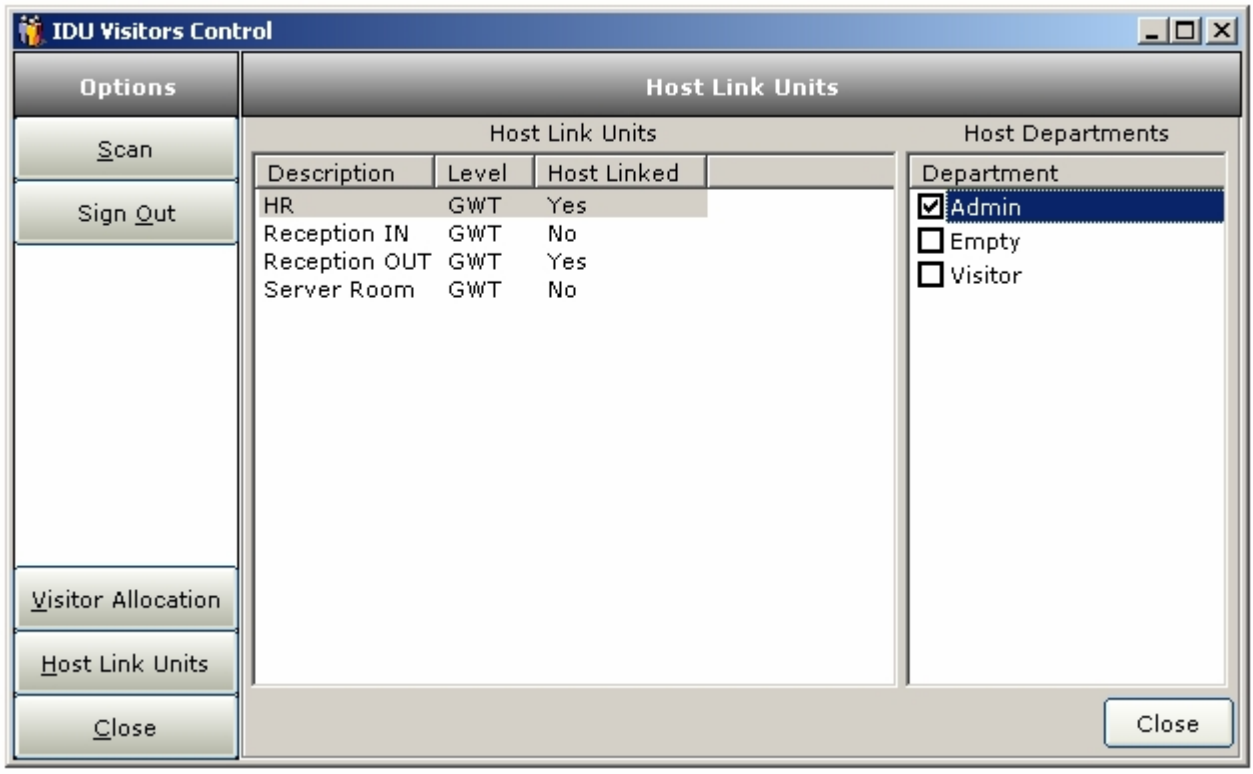
Sign In – Once enrolled and entered into the database, one can sign the visitor in by linking him to a host that has hosting rights. Important information like laptop and firearm serial numbers could be included if required.



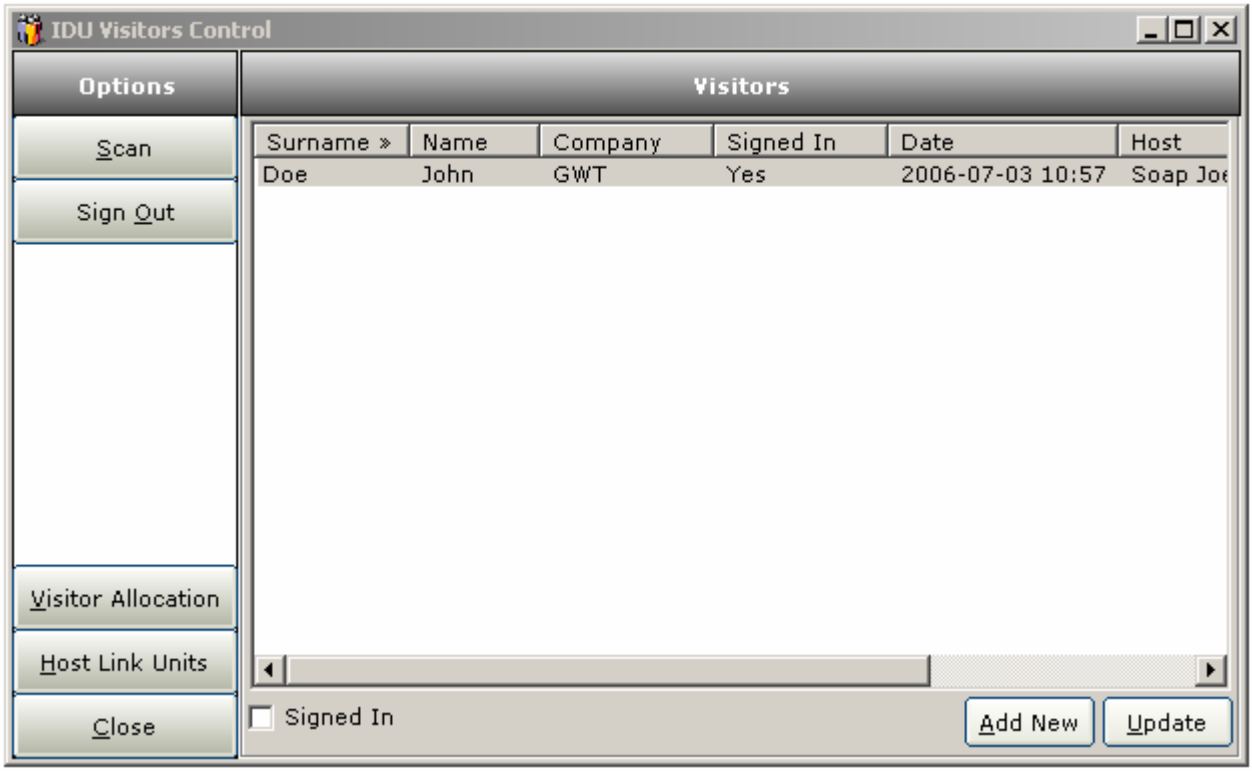
Visitor Allocation – Here you can define where visitors may have access or not. You can either select Allocate to Host's Readers (allow access to readers where host has access) or Allocate to Selected Readers (only selected readers).

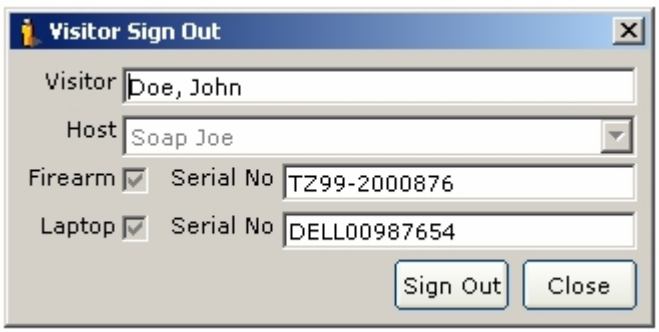


Host Link Units – You can define which readers are host grant readers (visitor presents finger, then host to grant access), and which are not (visitor has access without host). By double clicking the reader, its status changes to Yes, meaning that this particular unit is a host link unit. You can also select which department may host visitors, and will reflect in the Host area under the Visitor Sign In page.



Sign Out – Once a visitor is signed in and you need to remove him off the system, you can simply select the visitor and click on Sign Out. A confirmation page will appear, and you can click on Sign Out again.



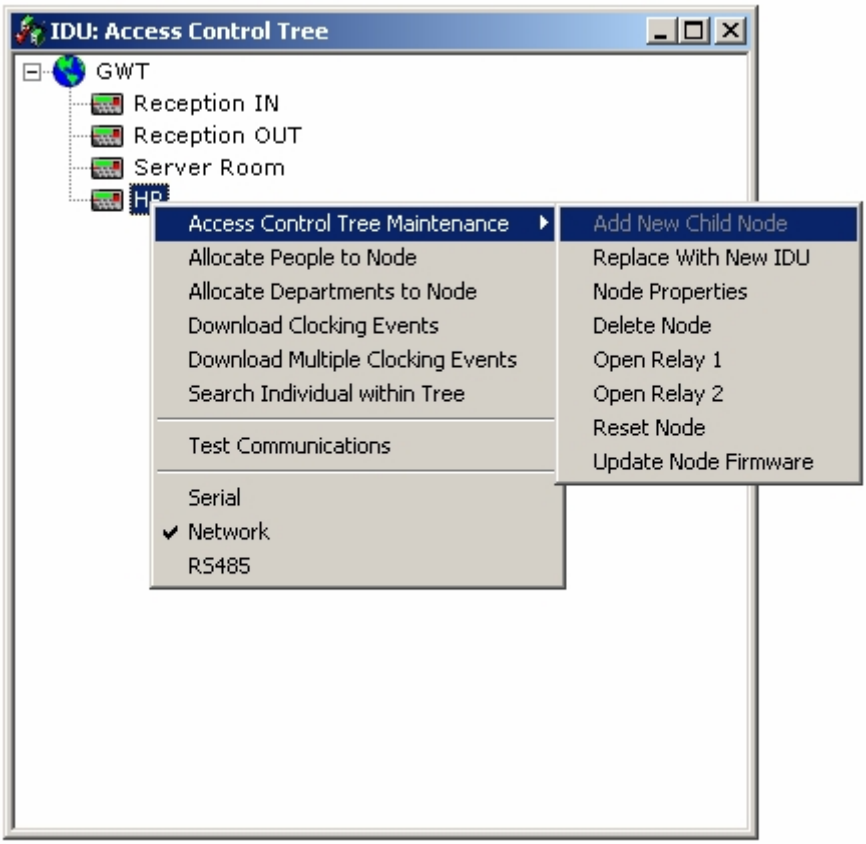


6. USING THE IDU ACCESS CONTROL SOFTWARE

Once the IDU ACCESS CONTROL Software has been installed and a user has logged in for the first time, the User Name and Password must be changed in the Application Security option on the IDU Access Control Menu. Click on **admin** in the Maintain Users Window and select **Update** to amend the user name and password.

6.1. Access Control Tree Menu Functionality

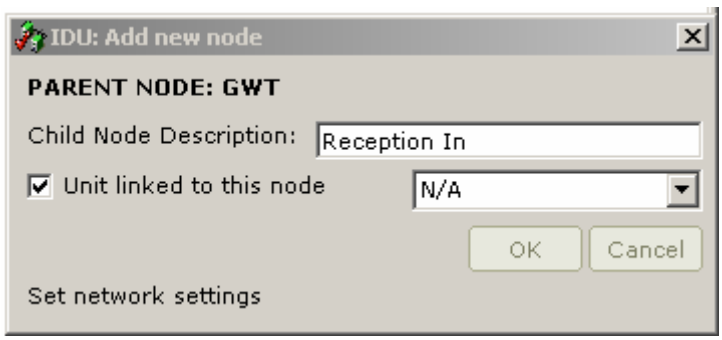
The Access Control Tree is the interface to all IDU devices, whether the device is connected via serial cable or on the network. Right click on any node to open a context menu pertaining to that node. A Child Node that is linked to an IDU device is indicated by an IDU icon.



6.2. Adding an IDU Device on the Access Control Tree

To add an IDU device to the Access Control Tree, first connect the IDU device to the PC with a serial cable and supply power to the device – this is necessary only for the first time in order for the application to read the IDU's unique serial number and MAC address. The application keeps track of which IDU belongs to which node for security purposes.

Select **Access Control** from the IDU Menu to open the **Access Control Tree** Window. Right click on the node in the Access Control Tree to which the device must be added. Select **Access Control Tree Maintenance**, and then select **Add New Child Node**. This will open the **Add new node** Window. Complete the relevant information and click the check box marked **IDU Unit linked to this node**. If a message box appears with the message "No communications with IDU device", ensure that the serial cable is connected, that the unit has power and that the correct serial port is being used. The default option for communication with devices will be changed to serial as devices cannot be added via the network – you have to configure the network settings via serial first, as will be seen in the IDU properties windows further down. Please note the difference between adding general nodes and one linked to an IDU is the check box being flagged.



The dropdown menu (combo box) indicates the use of the IDU device for time and attendance purposes and contains the following options: **(please note this setting does not influence**

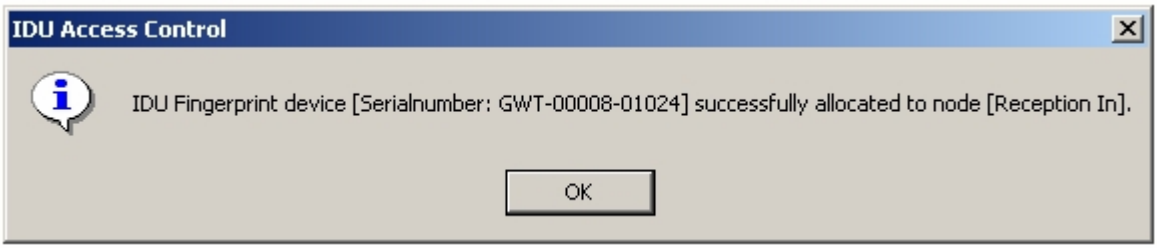
the operation of the IDU device at all – this is only a flag/indicator for when exporting date & time events to csv files. The application that imports the data must have the logic to interpret the flag)

The following flag values will be exported, together with other relevant data:

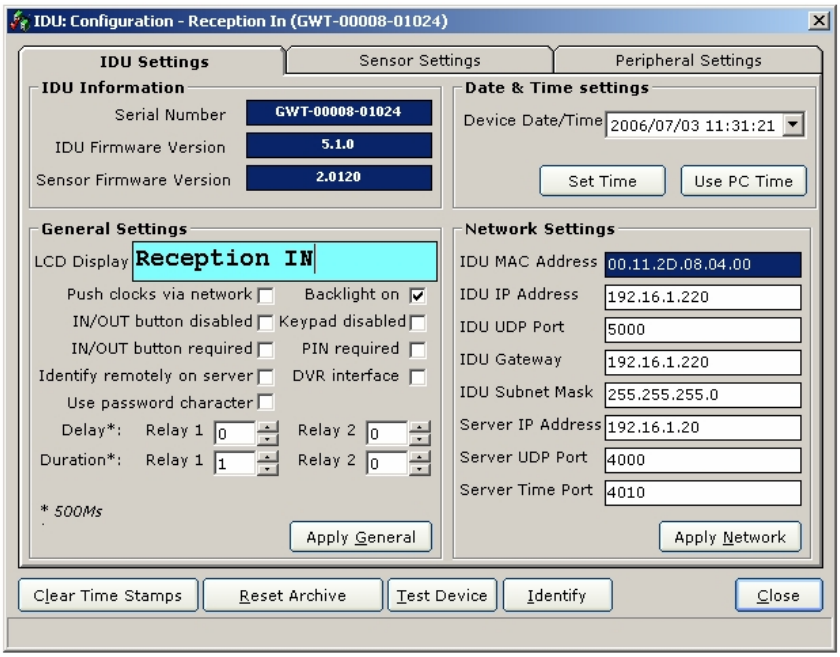
- **N/A = 0**
- **In = 1**
- **Out = 2**

Once the OK button is clicked the following window will appear, asking for the respective IDU to be connected to the pc via serial cable. (note all IDU devices comes with standard pre-packed serial cable)

After clicking yes the IDU unique serial is read from the device and allocated to the specific node within the Access Control tree – as per your specification. (note that you can only communicate with this IDU device by selecting the specific node that it has been allocated to – should you require to cancel the operation, please delete the node which will release the IDU against the node – you will also not be able to re-allocate this IDU against another node within the Access Control tree whilst it is already allocated against another node)

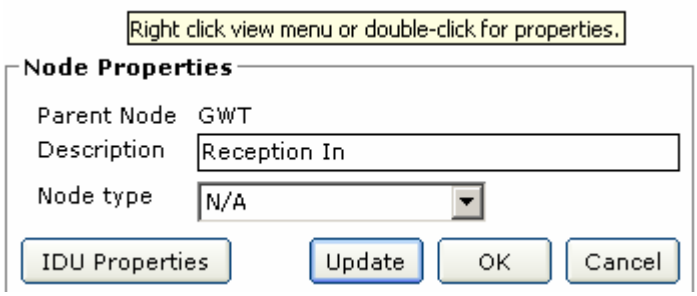


Automatically the "Node Properties" window appears, allowing configuration per IDU device. This section is addressed separately in the next point.

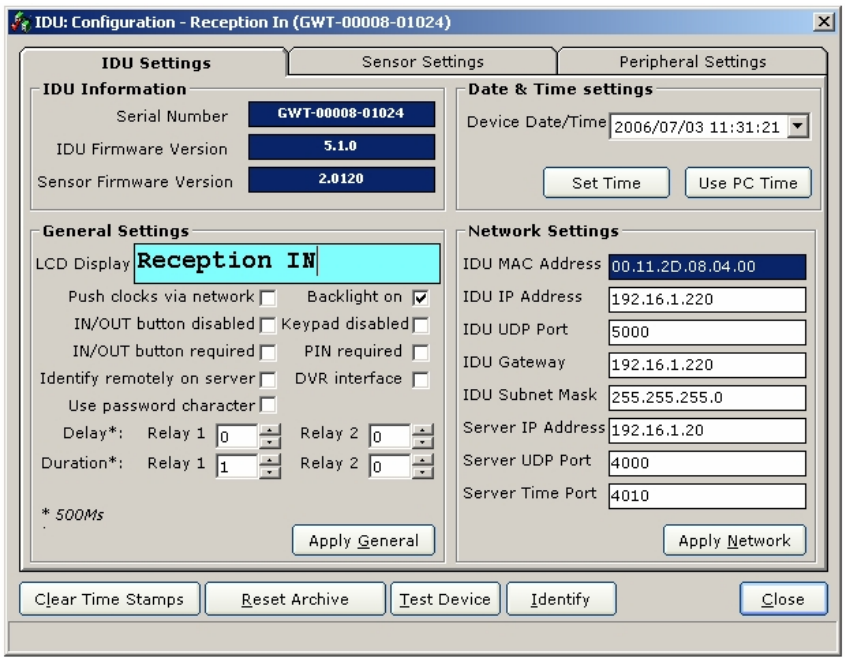


6.3. Node Properties

Note there is a difference between the properties of a general node (one not linked to an IDU device) versus one that is. Depending on the node that the cursor is on the context (pop-up) menu will enable or disable certain functions e.g. a node not linked to an IDU device will not allow allocation of people.



6.3.1. Node Properties - IDU Device



GENERAL SETTINGS (note the "Apply" button must be clicked in order for changes to take affect)

- **LCD Display:** This allows for setting the Liquid Crystal Display (LCD) on the IDU device
- **Push clocks via network:** Allows for interactive date & time clockings to be pushed via the network, note that the server side must be running in order to receive the clockings
- **Backlight On:** Switches the backlight on the LCD on or off
- **Keypad disabled:** Disables the keypad except for IN/OUT and Clear buttons.
- **In/Out Button:** This will enforce the in or out button to be pressed on the IDU before scanning a finger
- **PIN Required:** Allows for the IDU to always ask for a PIN code, implying always verification as opposed to identification. This allows for enhanced security without increasing security levels
- **Identify Remotely:** This setting will enforce VERIFICATION (Pin and Finger) and IDENTIFICATION (Finger only). The server in turn will do the relevant verification or identification and notify the IDU of a successful transaction or not.
- **DVR Interface:** After any identification the IDU will transmit a string (PIN, Name, Surname, Date & Time) via the serial cable - for example interfaces to flag DVR systems in displaying/recording the person's detail per identification or opening door
- **Use password character:** This will blank passwords out when using Pin and Password.

- **Relay delay:** This setting is indicated in 500 milli-seconds per each value of one. Allows for setting the duration in milli-seconds, after each successful identification, before sending electronic output signal. Please refer to technical specification – each IDU has two electronic signals out for interfacing into e.g. strike or magnetic locks e.g. The IDU device might not be mounted next to the door it opens – after scanning finger it might take the person 3 seconds to walk to door – this setting allows for mentioned time before sending electronic signal
- **Relay duration:** This setting is indicated in 500 milli-seconds per each value of one. Allows for setting the duration in milli-seconds, after each successful identification, of the electronic output signal. Please refer to technical specification – each IDU has two electronic signals out for interfacing into e.g. strike or magnetic locks

DATE & TIME SETTINGS

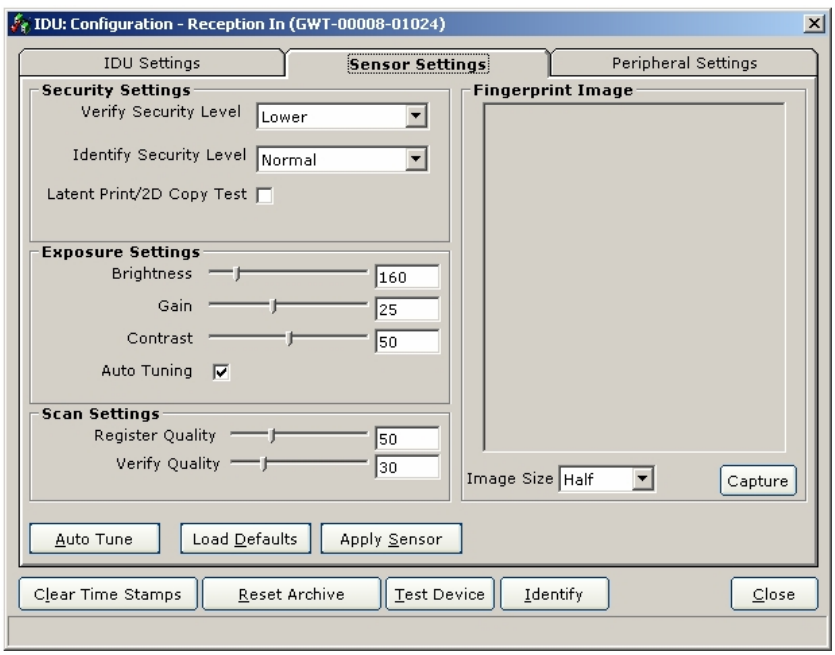
This allows to set the IDU device's date & time – for convenience one can only click on "Use PC Time" and the IDU device's date & time will be changed accordingly. A manual way of setting is also available.
The IDU device has an on-board real-time clock that lasts approximately ten years – Also due to non-volatile memory the device keeps **all** data in case of power failures.

NETWORK SETTINGS

The IDU unit has a network controller onboard and utilizes a TCP/IP stack to communicate, specifically the UDP protocol. Your network administrator should be able to give you all the information necessary to configure the unit.
Please note: The unit uses a static IP address, DHCP is not supported.

- **IDU IP Address:** The IP address of the unit
- **IDU UDP Port:** The UDP port that the unit will listen on for communications. When communicating with the device a combination of the unit IP address and UDP port will be used.
- **IDU Gateway:** The gateway address of the unit. If no router or such device are used the gateway address should be the same as the unit IP address.
- **IDU Subnet Mask:** The subnet mask for the IP address.
- **Server IP Address:** The IP address the unit will send packets to when pushing date/time clocks. This IP address is only used by the unit when communication is initiated by the unit, for ordinary communications the unit will reply to the IP address that initiated communications.
- **Server UDP Port:** The UDP port the server will use when sending commands to the unit.
- **Server Time Port:** The UDP port the unit will use when sending date/time clocks. The unit will use this port and the server IP address.

SENSOR SETTINGS



SECURITY SETTINGS: This section allows for increasing/decreasing of the security level. Verification is the 1:1 verification of a person, whilst identification is the 1:many identification. Herewith description of verification versus identification:

- Verification is where a person types in his/her PIN number and then presents the finger for scanning. This implies (should the IDU have 1,000 fingerprint templates on it) that the IDU will go directly to the specific/unique PIN and only verify the presented print against what is in the archive against the PIN;
- Identification is most commonly used where only a finger is presented – this implies (should the IDU have 1,000 fingerprint templates on it) it will go through all 1,000 and match the presented finger against the archive full of prints in order to identify the correct person.

- **Verify Security Level:** Security level setting for verification – suggested setting to start with is below normal. This should be increased should false acceptances occur.
- **Identify Security Level:** Security level setting for identification – suggested setting to start with is normal. This should be increased should false acceptances occur.
- **Latent Print/2D Copy Test:** Suggested setting is on - by enabling this setting the IDU will check for mentioned fake occurrences and not allow for positive identification.

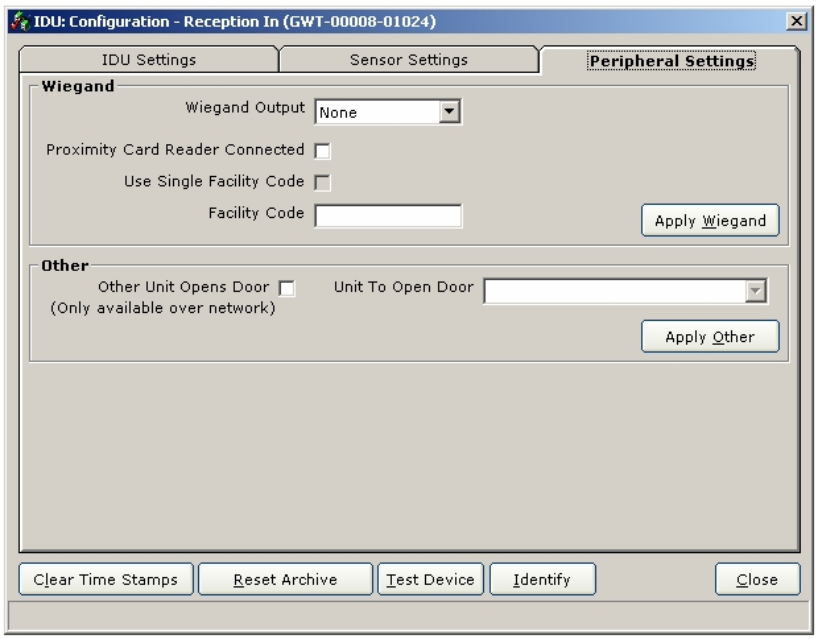
EXPOSURE SETTINGS: This section allows for manually & automatically fine tuning the sensor with regards captured images. **The suggested settings are contrast 50 and "Auto Tuning" enabled/checked.** As soon as auto tuning is enabled the brightness & gain settings will be disabled. By using auto tuning the IDU device will automatically optimize the quality of each and every fingerprint presented for scanning, as opposed to fixed brightness, gain & contrast settings – remember each and every finger differs.

SCAN SETTINGS:

- **Register Quality:** This setting allows for setting the minimum percentage quality for newly registered or enrolled fingers. Suggested setting is 50 and not below – should one drop to example 10 it will allow for bad quality fingers to be registered, influencing the identification process.
- **Verify Quality:** The minimum percentage setting for verification purposes, suggested setting is 30. Note that verification is more secure than identification and normally requires a lesser degree of security regarding matching fingerprints. (1:1 matching)

PLEASE NOTE DEFAULT SETTINGS COULD BE RESTORED BY CLICKING THE "LOAD DEFAULTS" BUTTON, THEN BY CLICKING THE "APPLY" BUTTON (this is the suggested setting)

PERIPHERAL SETTINGS



- **Wiegand output:** Select the protocol to use when sending Wiegand output. The options are none, 26 bit or 44 bit. When Wiegand output is selected the unit will send a Wiegand string when a person is successfully identified or verified with the person's PIN as value.
- **Proximity Card Reader:** This flag indicates, per IDU device, that there is a proximity card reader connected to the IDU device for verification purposes. Note that this setting does not influence the normal use of the IDU device, it only indicates that the device should also listen on the Wiegand port for a proximity card reader.
- **Use Single Faclity Code:** Only available when 26 bit Wiegand is selected. If this option is selected the unit will replace the entered facility code to the persons PIN (card number).
- **Facility Code:** Single facility code to use.
- **Other Reader Opens Door:** This flag indicates to the IDU device that another reader will open/interface to the door. This is an additional safety feature which allows for example the outside reader not to have any interface to the electronic door, implying that a reader on the inside of the building will interface and open the door. Should someone tamper or remove the outside reader, no electronic interface is exposed and the door remains safe. The reader to open the door can be selected from the drop-down combo box. This feature is only available via the network – this outside reader (after successfull identification) will notify the selected reader to open the door.

6.3.2. Reset Archive

This option deletes all the personal information stored on the archive of the IDU device – this includes fingerprint data & person text related data – excluding date & time events & IDU configuration settings.

6.3.3. Clear Time Stamps

This option deletes all date/time events stored on the IDU device. Any date/time events that have not been downloaded from the device will be deleted. It is not necessary to explicitly clear the IDU device's memory, as the date/time events are deleted when they are downloaded. This option excludes clearing fingerprint, person text data and IDU configuration settings.

6.3.4. Identify

This option identifies a person that has been allocated to the unit and retrieves the person's detail from the database. This option is only available via serial communication.

6.3.5. Test Device

This option performs error checking on the device with regards to the sensor, memory, etc. It will return an error should the device be faulty.

6.3.6. Capture

This option allows for capturing of images for viewing purposes – typically one can play/tune with the various sensor settings and capture fingerprint image for viewing. This is only available via serial – also the bigger the image requested the longer it takes (full, halve & quarter)

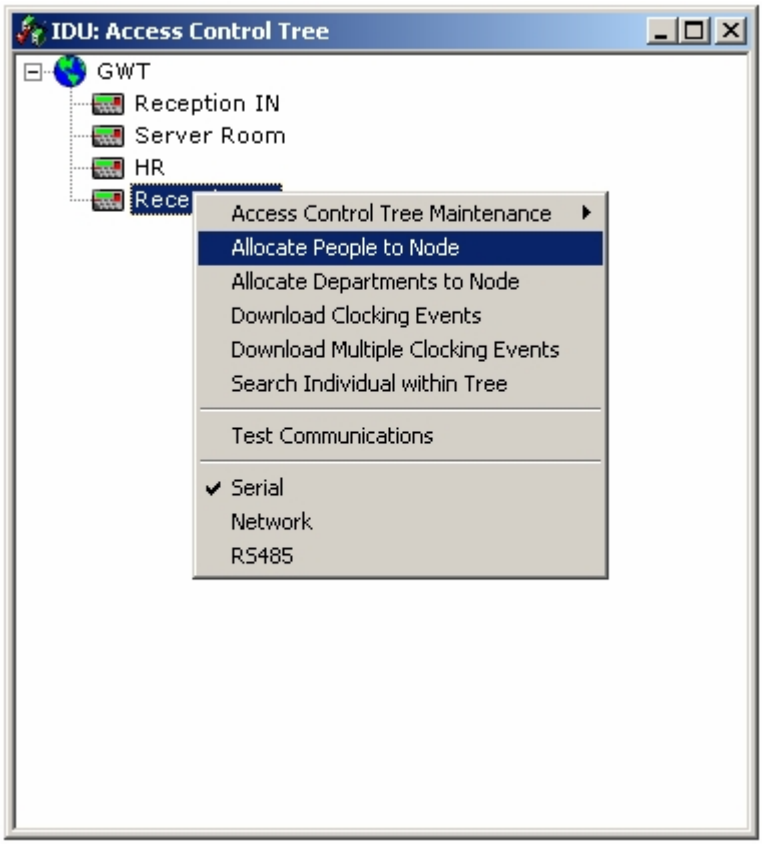
6.3.7. Close

Closes the **IDU Configuration** Window and returns to the **Access Control Tree** Window.

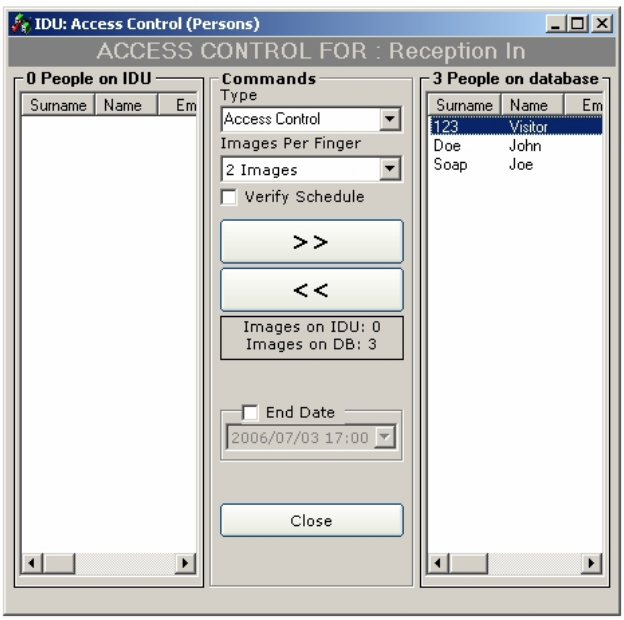
When all the necessary settings have been amended and applied, the IDU device can be accessed either through serial or network connection by right clicking on the relevant node in the Access Control Tree.

An IDU device cannot be moved from one branch of the Access Control Tree to another. To move a device, right click on the linked node. Select **Access Control Tree Maintenance**, and then select **Delete Node** to remove it from the Access Control Tree. Select the branch to which the IDU device must be moved and follow the above procedure to add the device as a new Child Node.

6.4. Allocation of People to IDU Device



Select **Access Control** on the IDU Menu to open the **Access Control Tree** Window. Right click on the node linked to an IDU device to which the people must be moved and select **Allocate People to Node**. Select whether to connect via the network or serial cable. This will open the **IDU Access Control (Persons)** Window.



People on IDU device: This indicates the number of people that have already been allocated to the IDU device.

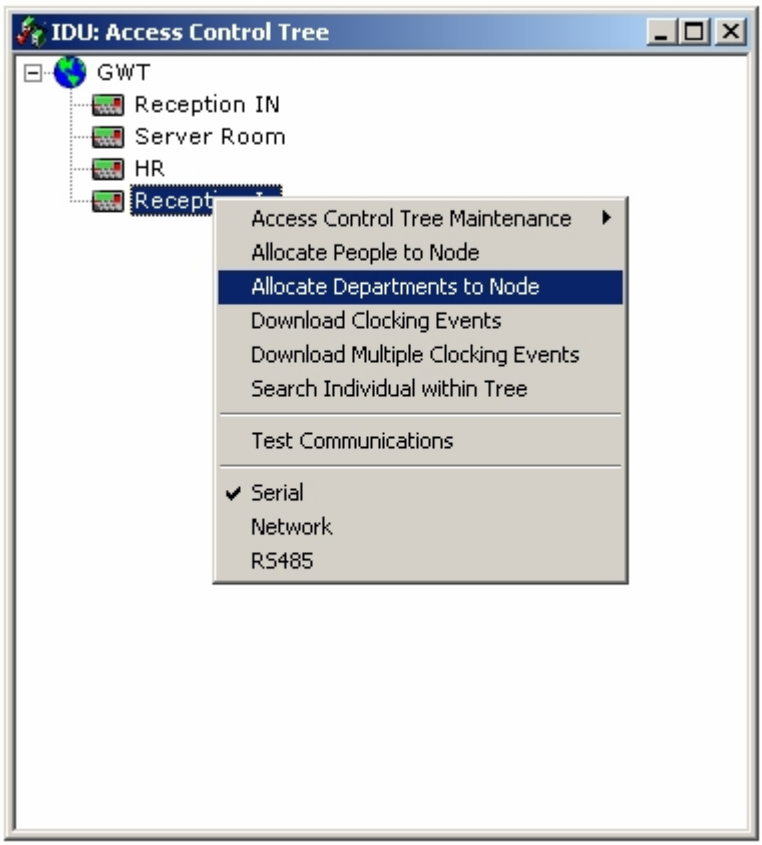
People on database: This indicates the number of people still on the IDU AccessControl database.

Usage: This option must be selected before people are allocated to the IDU device.

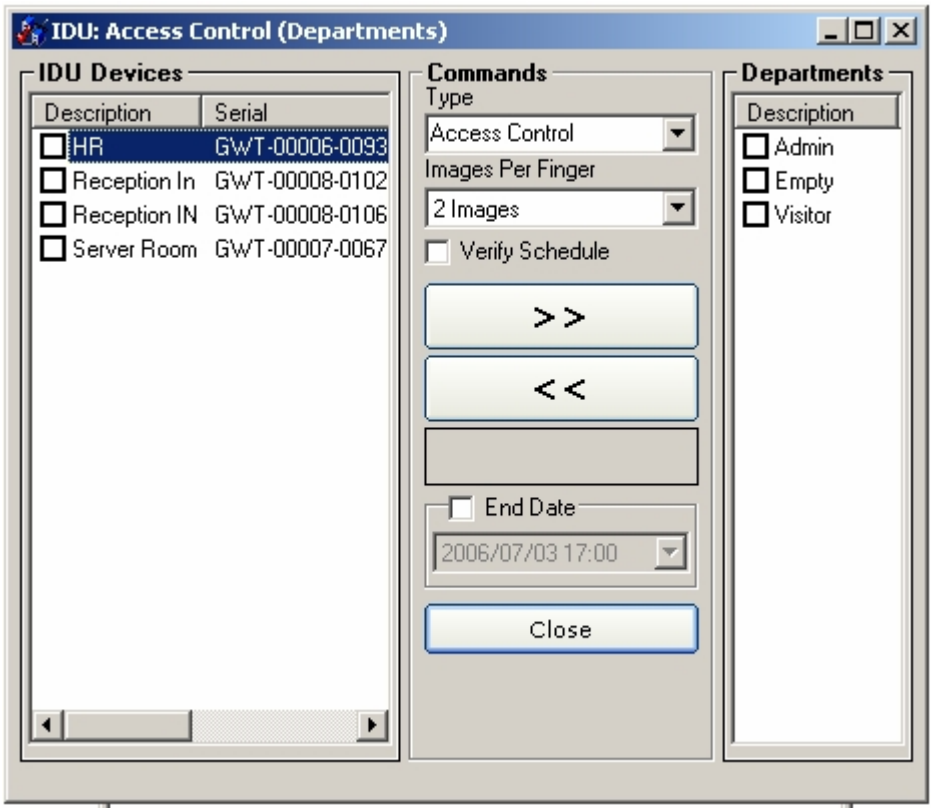
- **Access Control:** This option indicates that the IDU device, to which these people have been allocated, must trigger a relay on identification.
- **Time and Attendance:** The IDU device will not trigger the relay on identification, as it is used only to gather time and attendance records of employees.
- **Both (T&A and AC):** The IDU device is used for both functions and will trigger the relay on identification.
- **Verify Schedule:** This tick box should be used where schedules need to be linked to a certain individual or group of people before transferring their prints to a unit. This feature requires the **IDU Server** application to run all the time.
- **End Date:** This date is used to remove the person from a device via the **IDU Server** component.
- **Images Per Finger:** The number of images to transfer per finger.

>> / <<: Indicates the direction of the allocation. To remove people from the IDU device, select the people in the **People on IDU device** list box on the left, then select >>.The people will be moved back to the database. To allocate people to the IDU device, select the people in the **People on database** list box on the right and select << to move them to the IDU device.

6.5. Department Allocation to IDU



Select **Access Control** on the IDU Menu to open the **Access Control Tree** Window. Right click on the node linked to an IDU device to which the people must be moved and select **Allocate Departments to Node**. Select whether to connect via the network or serial cable. This will open the **IDU Access Control (Departments)** Window.



This functionality is only available via the network.

IDU devices: This shows the units available on the network. (allocated within Access Control Tree)

Departments: This shows the groups created in the system – when people were enrolled (added to the system) they were allocated to groups or departments.

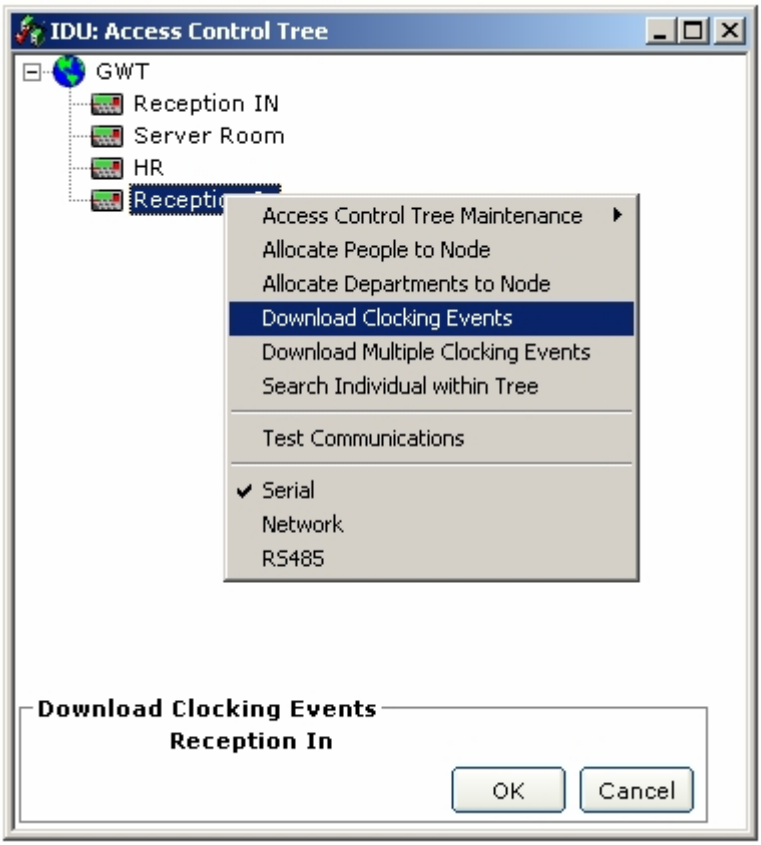
Select departments and IDU devices (nodes) for transfers ...

- **Access Control:** This option indicates that the IDU device, to which these people have been allocated, must trigger a relay on identification.
- **Time and Attendance:** The IDU device will not trigger the relay on identification, as it is used only to gather time and attendance records of employees.
- **Both (T&A and AC):** The IDU device is used for both functions and will trigger the relay on identification.
- **Verify Schedule:** This tick box should be used where schedules need to be linked to a certain individual or group of people before transferring their prints to a unit. This feature requires the **IDU Server** application to run all the time.
- **End Date:** This date is used to remove the person from a device via the **IDU Server** component.

>> / <<: Indicates the direction of the allocation. To remove departments or groups from the IDU device, select the group in the **Department** list box on the right, then select >>.The group will be moved back to the database. To allocate a group to a device, select the group in the **Groups** list box on the right, select the nodes which will be affected and select << to move them to the those devices selected.

6.6. Download Date/Time Events from IDU Device

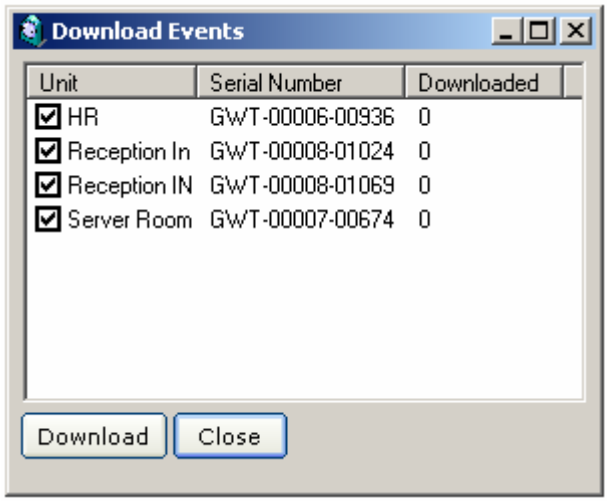
Select the **Access Control** option from the IDU Menu and right click on the node from which the date/time events are to be downloaded. Select **Download Clocking Events**, and then select the connection type (serial or network). The **Download Clocking Events** frame will appear.



Select **OK** to download date/time events. When the download is complete, a message box will indicate the number of events that have been downloaded to the database. The date/time events that have been downloaded from the device can now be exported to a .csv file. Note this action would also have cleared the downloaded events from the IDU's memory.

6.7. Download Date/Time Events from multiple IDU Devices

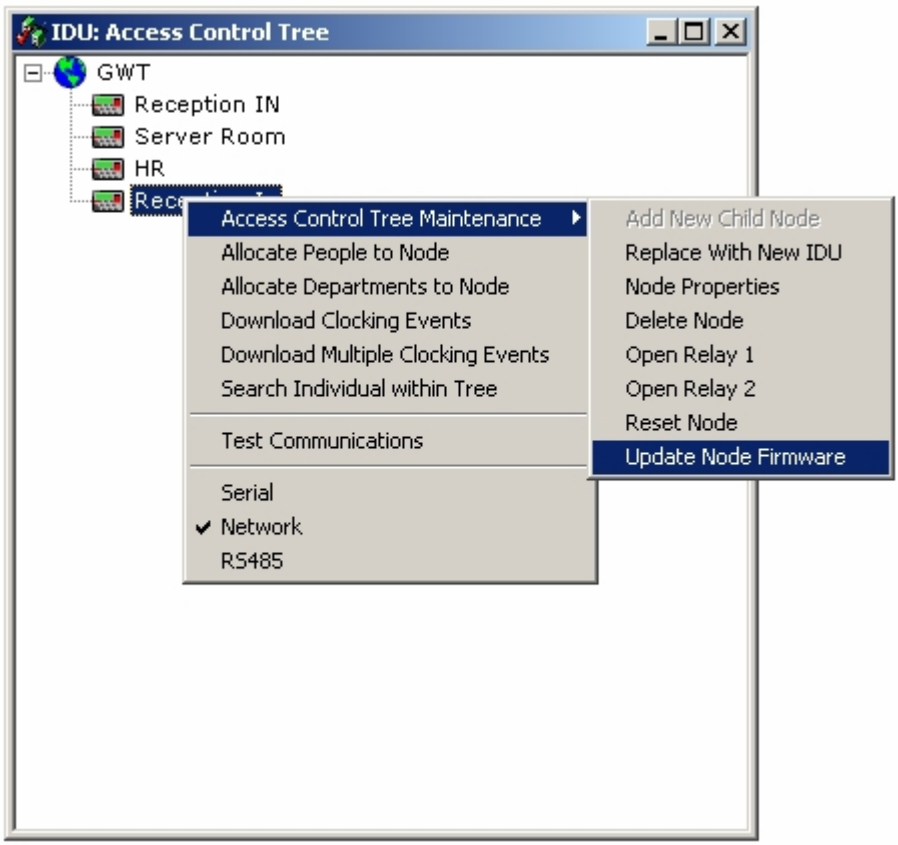
Select the **Access Control** option from the IDU Menu and right click on the node from which the date/time events are to be downloaded. Select **Download Multiple Clocking Events**, (this functionality is only available via network). The **Download Events** Window will appear.



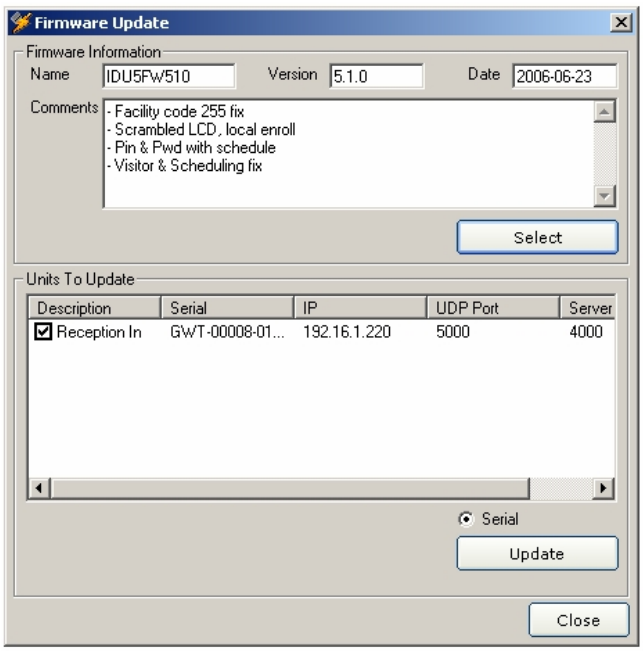
Select the devices to download date/time events for and click **Download**. When the download is complete, the default applications will be executed. If no default application has been setup a message box will indicate this. The **Launch** button will launch the default 'auto launch 'application as setup in the Options dialog.

The date/time events that have been downloaded from the device can now be exported to a .csv file. Note that this action would also have cleared all downloaded events from relevant IDU devices' memory.

6.8. Update Node firmware (Also see section 8)



When new firmware becomes available, use this functionality to update the software on each unit. Units can be updated via serial cable only. Click on select, browse to firmware file location, highlight correct firmware and click on open. Make sure you select the correct IDU from the list, connect the unit to the serial port, and click on Update.



7. INSTALLING THE IDU SERVER SOFTWARE

See paragraph **3. Installing the Access Control Software** (Custom Installation).

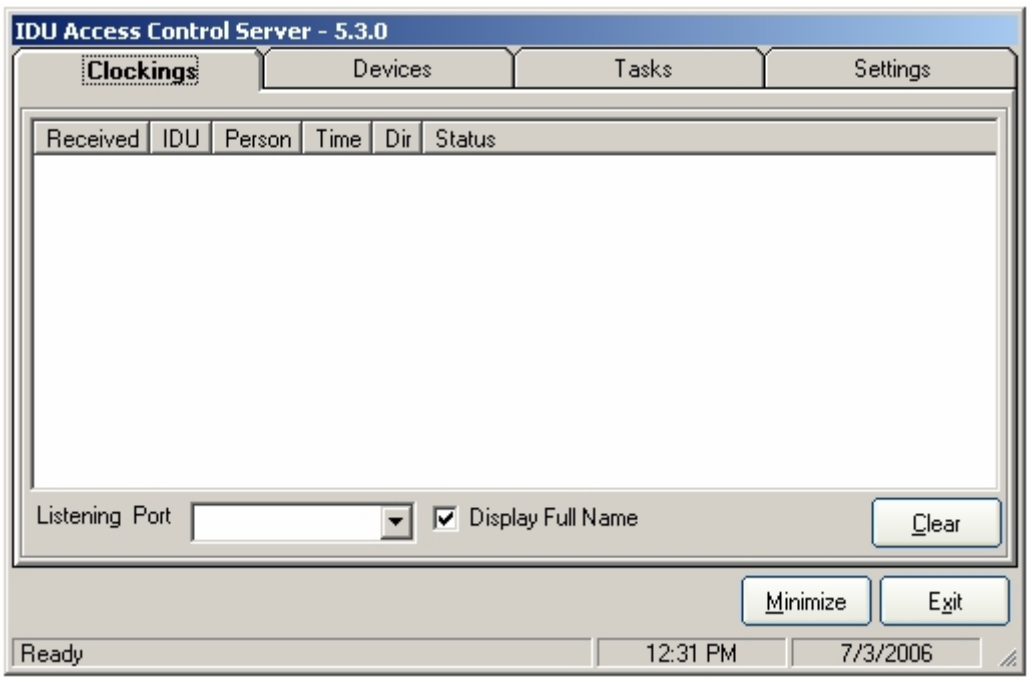
7.1. Using the IDU Server Software

The Server software if used in conjunction with units set up to push events in real-time via the network (refer to section 6.3.1) and also for units that has scheduling activated.

Online Identification and Verification also needs the IDU Server Software to run.

Open the Server application by double clicking the IDU Server icon.

7.2. Main form

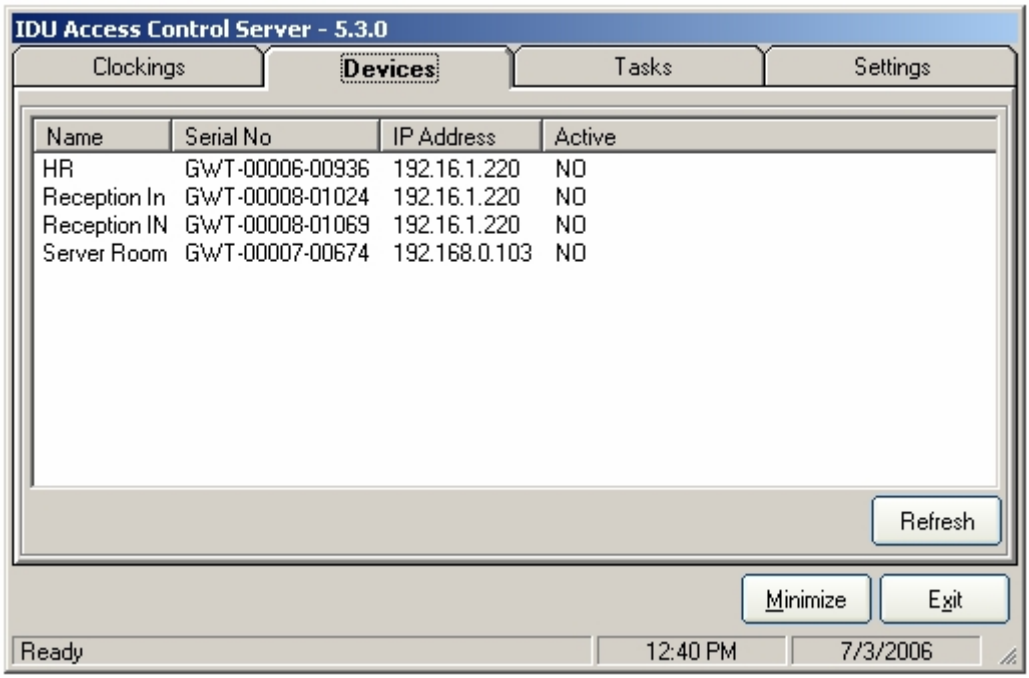


After **Minimize** has been clicked, the application sits in the icon tray. Double-click the icon to open the main form again.

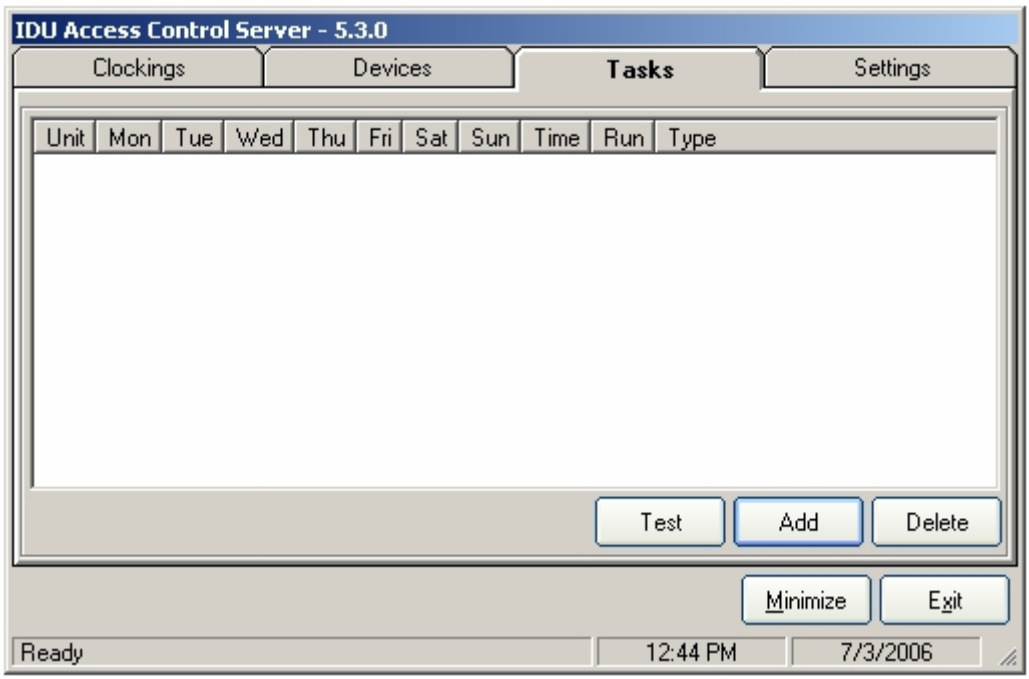
The combo box at the top displays all ports as setup for each device. Select one that the server will listen on for timestamps.

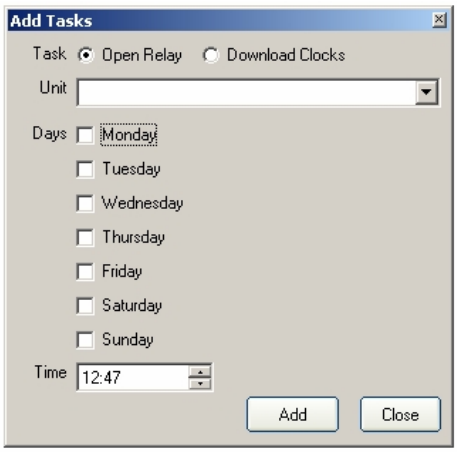
The **Clockings** tab will list all realtime clockings as received from units with Push Clocks Via Network enabled (see section 6.3.1). You can clear the current list of clockings by selecting **Clear** on the page. By having **Display Full Name** selected, the person clocking's name will be displayed and not the PIN.

Clicking on **Devices** will display a list all devices that the server has found to be available on the network. **Refresh** scans the network for available devices and re-populates the port combo box and devices list.

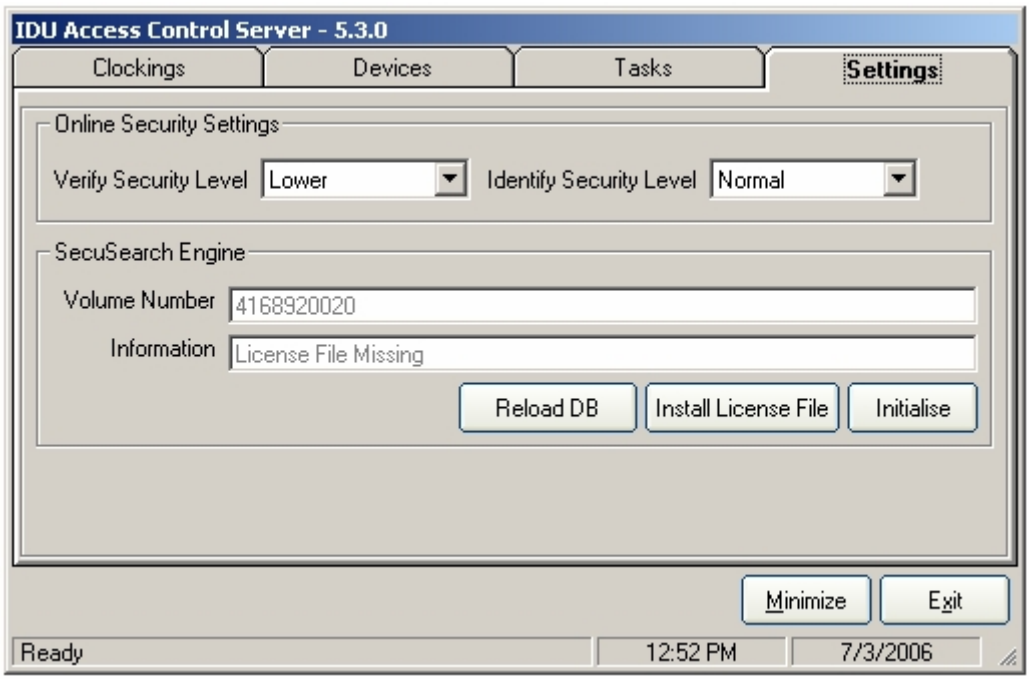


Tasks will allow you to schedule the opening of predefined relays or downloading of clockings in certain intervals (based in minutes). Click on Add to schedule a task.





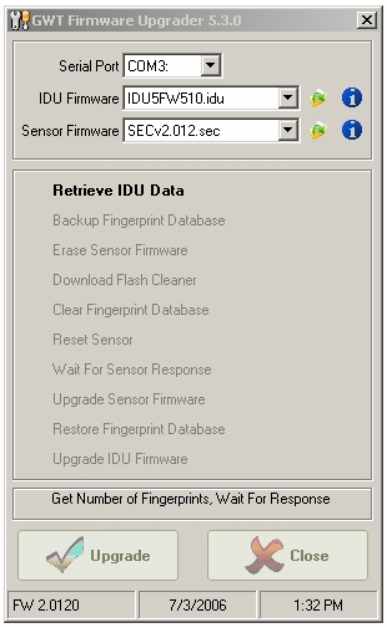
Settings tab will allow you to specify the Online Security Settings (see section **6.3.1 – Sensor Settings**), as well as licensing SecuSearch which is needed for Online Identification and Verification. A license file needs to be purchased from iPulse Biometrics to have this functionality operational (contact your account manager). After receiving your license file, click on **Install License File,** point to the file, **Initialise** it, **Reload DB** and open and close IDU Server. The SecuSearch Engine should now be started. Make sure you change the IDU settings as mentioned under section **6.3.1 - Identify Remotely on Server.**



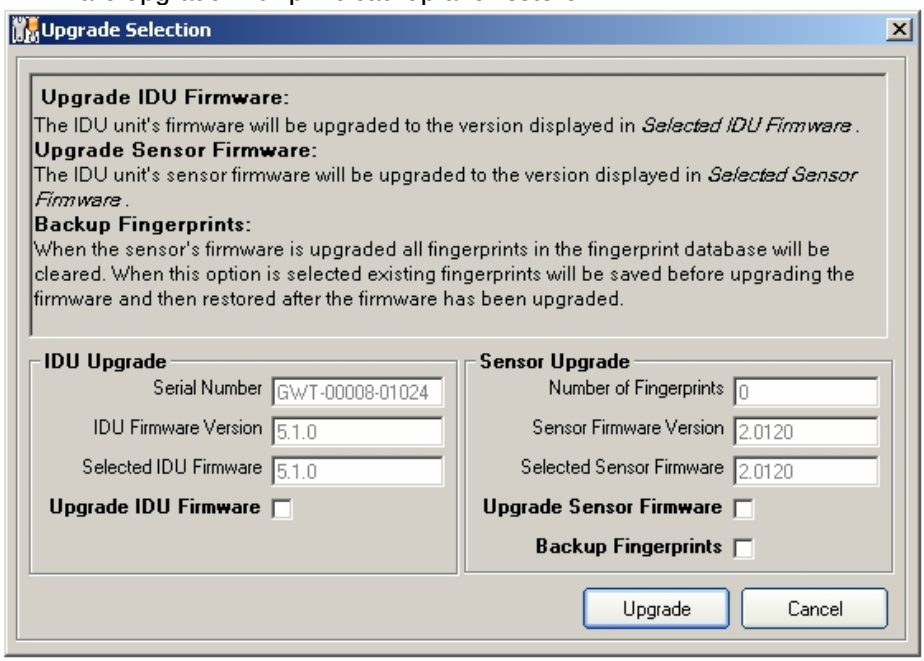
Exit closes the Server and **Minimize** hides the form and puts an icon in the tray.

8. FIRMWARE UPGRADE TOOL

The IDU Firmware Upgrade Tool installs automatically with a Typical installation, and can be found under Start-Programs-iPulse.



The IDU Firmware Upgrade Tool gives you more options when upgrading an IDU-5. Additional features include sensor firmware upgrade with print backup and restore.

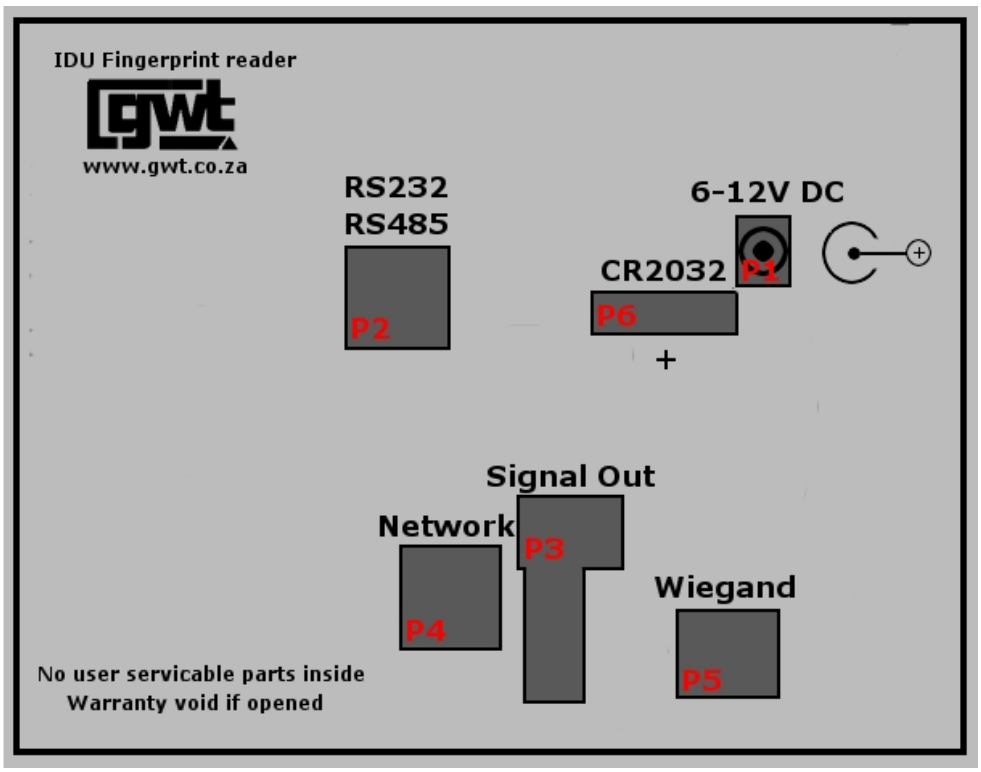


9. TECHNICAL DEVICE SETUP

9.1. Connector wiring

- P1 Power In
- P3 Relay Output
- P2 RS232/RS485
- P4 Ethernet
- P5 Wiegand IN/OUT

9.2. Back View and Connections



10. TROUBLESHOOTING & INFORMATIVE

10.1. Communication Problems

10.1.1. Serial Communication

- Check that all other programs that use the comport has been closed (e.g. Nokia 9210 Communicator)
- Check that the correct port is used (see 5.7)

10.1.2. Network Communication

- Check the network cable connected to the device for possible problems.
- Connect the device to the PC via RS232 and add to tree (see 6.2) and check that the network settings are correct.
- Reset the device or remove power from the device, then reapply.
- Ping the device to check whether it is available on the network.

10.2. Unit problems

LCD displays scrambled characters: Reset the device by right clicking on the relevant node in the Access Control Tree and selecting **Reset Device**.

On Selftest the LCD displays ID MOD NOT FOUND: Possible failure of component. Reset the device or remove power from the device, then reapply. If the problem persists, contact the supplier.

On Selftest the LCD displays ARCHIVE: FAILURE: Possible failure of component. Reset the device or remove power from the device, then reapply. If the problem persists, return the device to the agent.

LCD displays CLOCK ERROR: Possible failure of component. Reset the device or remove power from device, then reapply. If the problem persists, return the device to the agent.

Date and resets after power failure: The internal clock battery is faulty or has to be replaced, contact agent.

When power is applied to the device, nothing happens: Contact the agent.

10.3. Selftest and Reset

The IDU device performs a reset and selftest when the Clear button on the IDU face is pressed three (3) times.

10.4. Fingerprint Capture & Identification Problems

(This section courtesy of Secugen Corporation)

FAQs about Using SecuGen Sensors

---

1. How does fingerprint enrollment work?

When a three-dimensional fingerprint is applied to the sensor window of a SecuGen fingerprint recognition device, the fingerprint is scanned and a gray scale fingerprint image is captured. All fingerprints contain a number of unique physical characteristics called minutiae, which includes certain visible aspects of fingerprints such as ridges, ridge endings, and bifurcations (forks in ridges). Minutiae are generally found in the core points of fingerprints; core points are located near the centers of fingerprints. Figure 1 shows the positions of core points within fingerprints. The user is enrolled, or registered, in the database after a special minutiae-based algorithm extracts key minutiae points from the three-dimensional image at the time of acquisition (see Fig. 2).

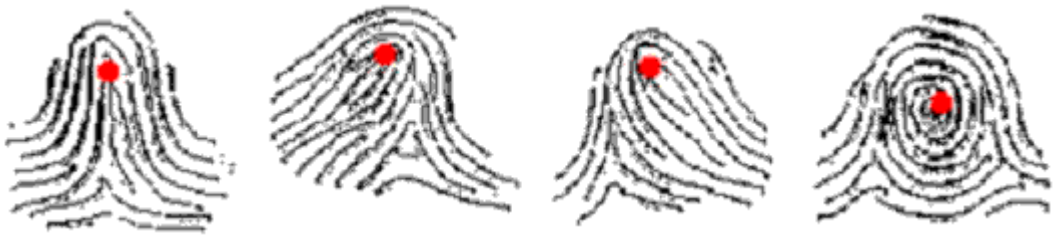


Fig. 1 Core points on different fingerprint patterns. A core point is defined as the topmost point on the innermost upwardly curving ridgeline.

Fig. 2 Examples of Minutiae

The extracted minutiae data are then converted into a unique digital template comparable to a 60-digit password. This unique template is then encrypted and stored. It is important to understand that no actual image of the fingerprint is stored, only the minutiae-based template. The process of enrollment actually takes two samples captured from the same finger before that finger is considered registered. When the next fingerprint image is captured during input, it is scanned by the fingerprint recognition device, converted to a template, and compared to the registered set for matching.

The term "biometrics" means the statistical use of measurable biological characteristics, like fingerprint minutiae. Biometric security, then, is based not on what you have (a key, a card) or what you know (a password, a PIN) - but who you are. Biometric security systems can be used in two distinct ways: (a) to verify a user's stated identity, or (b) to identify a user by finding the closest match in a database of stored fingerprint templates. The two methods are known as verification and identification, respectively.

The process of "authentication" refers to the validation of users on any system. Systems that use fingerprint biometrics include access control, time & attendance, and computer networks among many

others. Fingerprint recognition systems are used to authenticate people, and are ideal for supplementing or replacing simpler, less secure authentication methods such as passwords or IDs. Most experts agree that fingerprint recognition is the best of the various biometric techniques for its proven reliability, convenience, and cost-effectiveness.

Back

---

2. Why do I need to obtain good fingerprint images?

The quality of your fingerprint image is relative to the number of minutiae points captured. If the number and locations of the minutiae remain consistent whenever your fingerprint image is scanned and captured, your fingerprint image will successfully match the template of your registered finger. Fingerprint images that do not contain adequate minutiae data are not acceptable as personal credentials, and are therefore invalid. Figure 3 shows poor-quality fingerprints, characterized by smudged, faded, or otherwise distorted areas on the fingerprint. Conditions like these may be attributable to a number of factors, including excessively dry or wet skin, or scarring.

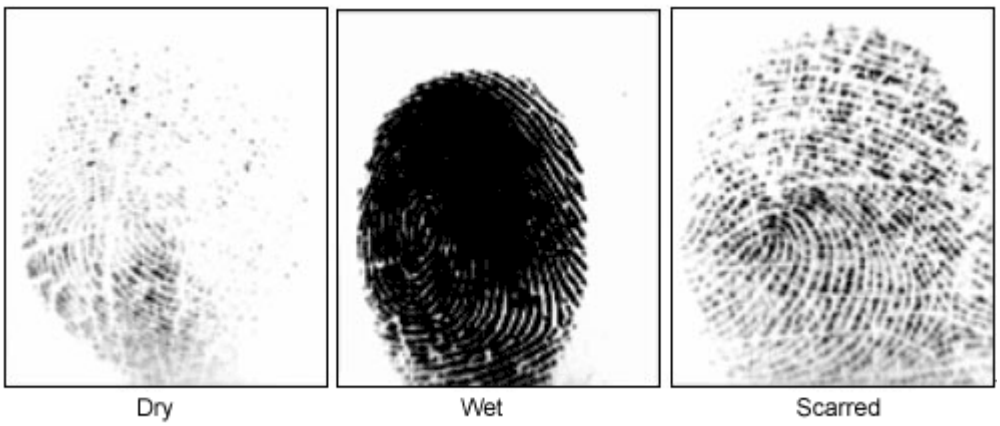


Fig. 3 Examples of poor fingerprint images

SecuGen's fingerprint matching algorithm is capable of extracting the correct minutiae even without benefit of a perfect print. However, the positioning of your finger and the relative wetness or dryness of your fingerprint when it is placed on the optic window for scanning are both important factors in getting a match. Bright lighting and humidity may also contribute to lowered performance if you are not careful. To minimize the chances of rejection by the system, especially in high security environments, you should know how to properly position your finger on the fingerprint reader. The best advice is to cover the optic sensor window completely with your finger to ensure that the maximum fingerprint surface area is exposed to the scan. A common mistake is to touch the sensor with the tip of your finger, which contains little or no usable minutiae.

Back

---

3. How do I correct problems from dry fingerprints?

When the temperature is low, or just after washing hands, the fingerprint is often dry. In this case, you may moisturize the fingerprint by breathing on it, or by touching your forehead to pick up surface oil before applying it to the sensor window.

Back

---

4. How should I position my fingerprint?

In order to capture the most minutiae, maximize the surface area of the fingerprint on the fingerprint input window by covering the sensor completely. It is okay for your fingertip to extend beyond the length of the sensor to center your fingerprint. Apply pressure lightly and evenly without moving it during the capturing process. Figure 4 shows the correct positioning of the fingerprint on the input window. Figure 5

shows the most common mistakes made during the initial phase of enrollment.

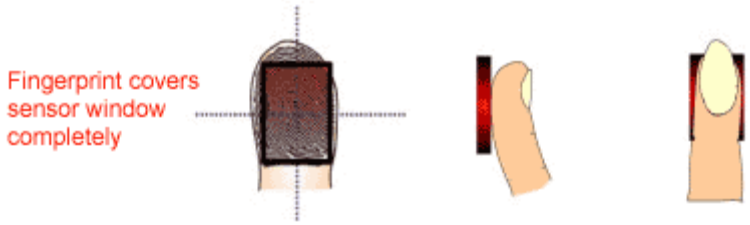


Fig. 4 Correct placement

Fig. 5 Common mistakes

Back

---

5. Why do I have to place my fingerprint twice during enrollment?

During enrollment, or registration, the process requires you to lift your finger from the device then put it back for a second capture. This second placement is needed because the registered fingerprint template is made from two samples. The method by which the system will ask you to do this varies depending on the kind of a device you're using. For instance, a PC peripheral device might make the request via a dialog window on your PC monitor, while a stand-alone unit for access control might display instructions to users on an LCD panel. Although the user interface may vary between applications, basic usage will be the same for any installation using SecuGen fingerprint readers.

Back

---

6. How much can I rotate my fingerprint?

For optimal speed in matching and verification, SecuGen's fingerprint system algorithm is set to allow up to ±45° for input fingerprint rotation, as illustrated in Figure 6.

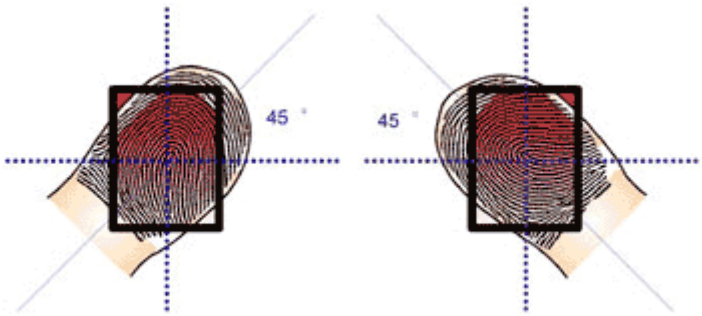


Fig. 6 The maximum angle of finger rotation

Back

---

7. How much pressure is required for a good-quality fingerprint?

If too much pressure is applied to the sensor window, the ridges may adhere to each other or become distorted. The net effect is similar to the hard-to-find minutiae of the wet fingerprint image because minutiae are rendered indistinguishable. On the other hand, if too little pressure is applied, the resulting image is similar to the dry fingerprint. Issues related to pressure are easily addressed, however. A little

practice is all that is needed for users to get the feel of it.

Back

10.5. Frequently Asked Questions (FAQ) about Biometrics

FAQs

---

1. What is biometrics?

Biometrics is an automated system of recognizing a person based on the person's physical or behavioral characteristics. It is the same system that the human brain uses to recognize and distinguish one person from another. It is a system that recognizes a person based on "who" the person is and does not rely on "what a person is carrying" or "what a person knows." Things that a person can carry, such as keys and ID-badges, can be lost, stolen, and/or duplicated. Things that a person knows, such as passwords and pin-numbers, can be forgotten, stolen, and/or duplicated. Instead, biometrics relies on "who" a person is-on a unique immutable human characteristic that can not be lost, forgotten, stolen or duplicated. Biometrics, therefore, provides the ultimate level of security, convenience and ease of use. It is this security and convenience that SecuGen's fingerprint recognition system provides.

Back

2. What applications can use fingerprint recognition?

As many as the imagination can hold. Fingerprint recognition can be used in any application that requires security, access control, and identification or verification of the user. These applications include PC-peripherals for secure workstations, PC network security solutions, E-commerce, entry-access systems, door-locks, time-and-attendance machines, ATMs, toys and games. Presently, SecuGen's technology has been successfully integrated into computer mice and keyboards, network security solutions, Internet security solutions, on-line banking systems, door locks, access control systems, time & attendance machines, and ATMs. These products have proven performance and are sold throughout the world.

Examples of **hardware** products developed using SecuGen technology.
Examples of **software** products developed using SecuGen technology.

Back

3. What is the difference between verification and identification?

Fingerprint recognition methodology is divided into two distinct processes: Verification and Identification. The Verification process is a one-to-one matching process (1:1). The user states who the user is. A new fingerprint sample is taken from the user and compared to the user's previously registered or stored fingerprint. If the fingerprints match, the user is "verified" as who they say they are, and granted all the privileges and access of the stated user-the system verifies who the user says they are. The Identification process is a one-to-many matching process (1:N). A user need not state who they are. A new fingerprint sample is taken from the user and compared to a database of existing fingerprints of registered or stored users. When a match is found, the user is "identified" as the preexisting user-the system finds who the user is. This one-to-many matching process is how the Automated Fingerprint Identification System (AFIS) works. SecuGen offers both verification and identification technology.

Back

4. How do SecuGen's fingerprint recognition products work?

First, a user must enroll their fingerprint for future verification (1:1) or identification (1:N). A user can enroll by placing their finger on a SecuGen® fingerprint recognition device such as a SecuGen® Mouse or an access control device integrated with a SecuGen fingerprint module. The device sensor scans the user's finger and captures the live 3-D fingerprint image. SecuGen's minutiae based algorithm then extracts minutiae points from the image and converts the data into a unique mathematical template, comparable to a 60 digit password-a password. This unique template is then encrypted and stored to represent the user. No actual image of the fingerprint is stored.

Next, for verification, an enrolled user states who they are (i.e. enters a user ID) and places the his or her finger on the device sensor. A new fingerprint image of the user is captured. Minutiae data is extracted from the fingerprint and converted into a template. This template is then compared to the user's pre-enrolled template for a match. If the templates match, the user is verified positively. For identification, a user places the his or her finger on sensor without stating their identity (i.e. does not enter any user ID). The newly extracted template is then matched against preexisting templates. If there is a match, the user is identified as the user who enrolled the preexisting template.

Back

5. Why does SecuGen focus on fingerprint technology as opposed to other types of biometrics technology?

Considered the oldest and most commonly accepted form of biometrics, fingerprints have been used for verification and identification purposes for thousands of years. Both the United States and Europe began documenting the use of fingerprints for identification and verification over a hundred years ago. After all this time, and millions of fingerprints later, no two identical fingerprints have ever been found. It is safe to say that fingerprints are truly a unique human characteristic, as no other biometrics technology can boast this level of scientific history and evidentiary support. Accordingly, its advantage over other biometric solutions lies in its proven accuracy, reliability, convenience, user acceptance and familiarity. Moreover, with SecuGen's technology and through support for developers, many applications have been developed and many more are continually being developed to make fingerprint recognition systems useful and affordable for consumers everywhere.

Back

6. What are the benefits of using biometric identification rather than conventional methods of security such as passwords, pin-numbers, physical-keys, access codes, or key cards?

Imagine if you will, starting your morning by pressing your finger on SecuGen's fingerprint recognition sensor to turn off your alarm clock. The alarm clock gives you a morning greeting by name. The house begins to awake, as it knows you are up. Instantly, the coffee begins brewing to your preset specifications and the shower is set to the water temperature of your liking. When you get out of the shower and begin dressing, the TV turns on to your favorite morning show. As you leave your house, you

press your finger on SecuGen's fingerprint door-lock and the house is automatically locked and secured and all appliances turn off-no keys to carry or lose. Multiple attempts to open the door by anyone other than a registered user will automatically summon the police. Likewise, if so programmed, the police will be automatically alerted if anyone with outstanding-warrants or anyone listed-on any police wanted-lists attempts to open the door. You can even check when and how many people came to the house when you return home or from your office through the Internet.

Next, you go to your car and with another press of you finger the door is opened. The car seat automatically adjusts to your settings and a gentle voice greets you by name. A press of your finger starts the car and the radio begins playing to the tune of your favorite station.

When you arrive at your office, a press of your finger gives you access to the parking lot and your office building-no access cards or ID badges to carry. Your presence is automatically notified to all your business team members and assistants should they need to talk to you. You start your computer and the network log-on screen comes on. You simply place your finger on a SecuGen® Hamster and you are granted immediate access to your computer and your office network-no passwords to memorize or write-down on yellow sticky paper. Whether on the intranet or on the Internet, with SecuGen's fingerprint recognition system, you, your company, and those you interact with on the Information Highway feel secure knowing you are who you say you are and not an impostor. Workflow is immediate and can be truly paperless when document authentication can be done over cyberspace.

For lunch, you realize you don't have enough cash, so you stop by a local bank. You approach the ATM machine powered by SecuGen technology and with another press of your finger, you have instant access to your bank account.

Imagine... A world without cumbersome keys, access cards, ID-badges or a need to memorize numerous passwords, pin-numbers or access codes. A world that is more secure and convenient for you and your future generations. These are examples of the many benefits of biometrics and what SecuGen can offer. These benefits are not a dream but a reality of what SecuGen can provide today. The scope of these benefits are bound only by your imagination.

Back

7. How do SecuGen's products handle dirt, oil or moisture buildup?

Very well. SecuGen's optical prism is specially designed to resist distortions caused by dirt, oil or moisture buildup. Unlike many other optical devices, there are no expensive coatings to disturb on the hard surface of the prism. Designed for high usage and daily exposure to touch and contaminants from hands, SecuGen's rugged and scratch-resistant fingerprint sensor can easily be cleaned or wiped with a cloth or household glass cleaner if necessary.

Back

8. What are the advantages of SecuGen's optical fingerprint recognition technology over semiconductor (or chip) -based technologies?

Physical strength. SecuGen's optics-based system is physically stronger than semiconductor-based systems in terms of impact-resistance, scratch-resistance, weather-durability, and corrosion-resistance. Physical strength is a key factor for versatile outdoor usage. Semiconductor-based systems must apply special surface treatments to protect their inherently weak surfaces. Even then, they are far weaker than SecuGen's optical-prism strength.

Low maintenance costs. Semiconductor chip-based fingerprint recognition systems have higher maintenance costs than SecuGen's system due to their fragility. Unlike SecuGen's optical system, semiconductor-based systems use fragile and expensive parts that are equally expensive to replace and maintain.

No electrostatic problems. Semiconductor systems are inherently susceptible to damage from electrostatic energy, especially in carpeted areas. SecuGen's optical system is immune to electrostatic

energy. Static electricity can actually burn out an entire semiconductor-based system.

Back

9. What are the advantages of SecuGen's fingerprint recognition products over other optics-based fingerprint recognition systems?

High image quality. Traditional fingerprint devices require fine hand-calibration of its optical components. As such, image quality can vary significantly from one unit to another depending on the level of calibration. Accordingly, mass production of such units is costly or nearly impossible. Furthermore, such systems cannot endure high physical impact or shock, limiting their potential for outdoor use. SecuGen's patented-pending optical system allows mass production of high quality image capturing modules with minimal calibration requirements. Additionally, conventional optical fingerprint recognition systems use FTIR (Frustrated Total Internal Reflection) image processing methodology. In such systems, high image quality requires longer focal lengths and therefore longer and larger modules. To make these conventional optical systems smaller, image quality must be compromised and the system is left to work with inherently distorted images. Image distortion effectively lowers accuracy and reliability. By contrast, SecuGen's Fingerprint Recognition System utilizes a unique, patented SEIR (Surface Enhanced Irregular Reflection) imaging method. Using this breakthrough technology, SecuGen's fingerprint modules are able to achieve distortion-free image capturing while drastically reducing its physical size.

Compact size. In traditional optical systems, higher image quality means longer focal lengths, which in turn means larger devices. SecuGen's patented-pending optical system provides distortion-free high image quality in the most compact module-design available today.

Resistant to grease and oil buildup Image quality is reduced when grease or oil builds up on the optical surface. Unlike other optical systems, SecuGen's patent-pending optical prism does not allow for grease or oil to build up on its surface. In addition, SecuGen's patented- pending optical prism is highly resistant to abrasions and is nearly indestructible.

Performs well under extreme conditions. Unlike other optical systems, SecuGen's fingerprint recognition system can operate under extreme temperature and humidity. Due to its superior wear-resistance, SecuGen's optical system functions well even under the most difficult outdoor weather conditions.

Low Cost. SecuGen offers the most cost-effective fingerprint recognition solution with the highest image quality available in the market today. SecuGen's advanced automated manufacturing processes mean reliable mass production. The result is a tremendous value to our customers at a significantly reduced cost.

Back

10. How fast can SecuGen's products verify a user?

The verification speed is generally less than half a second.

Back

11. What are the False Rejection Ratio (FRR) and False Acceptance Ratio (FAR) of SecuGen's products?

The False Rejection Ratio (FRR) states the percentage of instances an authorized individual is falsely rejected by the system. In general, SecuGen's False Rejection Ratio is 0.1%. The False Acceptance Ratio (FAR) states the percentage of instances a non-authorized individual is falsely accepted by the system. In general, SecuGen's False Acceptance Ratio is 0.001%. FRR and FAR are diametrically opposed. Therefore, raising the FAR will lower the FRR and vice-versa. Accordingly, FRRs and FARs can be adjusted according to need to fit the requirements of an outlying security system. SecuGen software products offer 9

different security levels that allow you to adjust the FRRs and FARs to reach the desired results.

Back

12. How well do SecuGen's products capture dry fingerprints?

Unlike other optical systems, SecuGen's SEIR (Surface Enhanced Irregular Reflection) optical technology combined with SecuGen's proprietary algorithm is able to capture extremely high quality, accurate, and distortion-free images. SecuGen's optical system is thereby able to capture even the driest fingerprint images that other optical systems can not.

Back

10.6. Secugen Technology

About SecuGen Technology

---

1. Why fingerprints?

Fingerprint biometrics represents over 50% of all biometric methods in use today. A mature and well-developed technology fostered by healthy competition among many biometric technology providers, fingerprint recognition is considered the best choice for many applications because of its accuracy, speed, reliability, non-intrusive interfaces, and cost-effectiveness.

2. SecuGen's core technology

SecuGen's core technology is designed into a revolutionary, patented optical module that works with a powerful set of extraction and matching algorithms developed for use with the unique SEIR optical method. The module is embedded in SecuGen's line of fingerprint PC peripheral devices and stand-alone devices used by OEMs around the world for applications such as access control and time & attendance. Software is available for desktop computer users, networks, and the Internet serving a variety of needs.

3. SecuGen's SEIR Optical Method

Fingerprints can be scanned in different ways. Current techniques include optical, ultrasound, and technologies based on semiconductor chips.

SecuGen has pioneered the Surface Enhanced Irregular Reflection (SEIR) optical method and patented technology, resulting in the most compact and durable optics-based fingerprint recognition systems in the world.

The scratch-proof platen of the patented optical module is another first in the industry; as hard as quartz, the sensor surface requires no special coatings or maintenance and is virtually unbreakable.

The robust hardware extends the lifetime of SecuGen products far beyond any chip-based fingerprinting technologies and is easily small enough to embed into consumer devices.

4. SecuGen's Optical Method vs. Semiconductor (Chip) Method

5. How it Works

At the most basic level, all optics-based fingerprint systems translate illuminated images of fingerprints into digital code for further software processing, e.g. enrollment (fingerprint registration) and verification (authentication of registered users).

SecuGen devices use the advanced SEIR method and CMOS image sensor to capture high contrast, high resolution fingerprint images that are virtually distortion-free.

A series of powerful algorithms developed by SecuGen extract minutiae data from the image, mapping the distinguishing characteristics of fingerprint ridge ends, splits, dots, and arches. Other fingerprint minutiae include whorls, loops, ridge lines, valleys, bifurcations, upper and lower cores, and deltas.

This data is then converted into a digital template (around 400 bytes) and stored in memory or on disk. (The actual fingerprint image is never stored, and cannot be constructed from templates.)

To identify or verify a fingerprint, a proprietary matching algorithm compares the extracted minutiae points from the input fingerprint to a previously stored sample. The entire matching process takes roughly one second. Authentication takes place either locally or on a server, depending on system configuration.

6. Fake or spoofed fingerprints

SecuGen devices also protect against latent fingerprints left on the sensor surface and "faked" 2-D fingerprints, such as photocopies or photographs. Constantly striving for innovation and meeting customer demands, SecuGen continues to research and develop new methods to counteract spoofing attacks, features once considered the exclusive domain of expensive and highly specialized ultrasound technologies.

10.7. Why choose Secugen Technology

(This section courtesy of Secugen Corporation)

Top 5 Reasons for Choosing SecuGen

#1. SecuGen sensors are amazingly durable and maintenance-free

The SecuGen sensor is well-known for its ruggedness and solid engineering, as well as its virtually indestructible sensor prism, which is made of a very hard quartz-like material that resists scratches, stress and corrosion.

From the sensor surface to the internal lens and electronic components, all aspects of the SecuGen sensor were carefully designed and redesigned to work reliably and consistently for even the most demanding applications.

SecuGen sensors were tested under extreme conditions and have been proven to perform in high-traffic, outdoor and other rough environments. They resist exposure to:

- Subfreezing, arid, and tropical climates
- Electrostatic discharge (ESD)
- Impact, vibration, and shock
- Scratches to sensor prism even from sharp objects
- Contaminants and corrosives such as sweat, dirt, oil and cleaning agents

SecuGen sensors do not use any coatings or thin films, which are required by many semiconductor-based sensors and competitive optical sensors in the market in order to protect the delicate sensor components or to improve contact with the skin. Such coatings may be vulnerable to scratches and corrosion that can degrade the performance of the sensor over time and cause unexpected replacement or repair costs in the long run.

Additionally, the optic parts are tightly assembled so that if the sensors are ever dropped, there is no need for re-calibration, which is often necessary for smaller form-factor optical sensors that use an intricate arrangement of mirrors or lenses.

#2. SecuGen sensors are very accurate

SecuGen sensors produce very high accuracy rates. In an independent test of major biometric products, carried out by International Biometric Group, SecuGen's sensor and algorithm achieved 0.0% false acceptance and 0.0% false rejection rates.

An innovative optic design yields practically distortion-free, high-contrast images from which data points are used for enrollment and matching. SecuGen's patented SEIR method eliminates the majority of

distortion and image quality problems that are common to traditional optical sensors.

High quality images mean greater precision, less false rejection, less false acceptance, and better overall performance.

#3. SecuGen sensors have the best quality guarantee and warranty in the industry

SecuGen sensors are made with advanced quality control techniques that further enhance the quality workmanship and materials that go into every single sensor.

If there is any defect or fault in the performance of a SecuGen sensor product, we will gladly replace it for free within one year of purchase. SecuGen is committed to proactive, ongoing improvements in product development, manufacturing and QA processes with the goal of making the best quality fingerprint sensor in the market for all uses.

#4. SecuGen sensors are used all over the world

Years of real-world use, integration into thousands of products, and use by real-world people have all proven the quality and reliability of SecuGen sensors.

SecuGen's customers come from nearly 50 different countries and include Fortune 500 companies, leading security and biometric companies, original equipment manufacturers, and government, financial, educational, and health care organizations.

#5. SecuGen sensors are supported by a wide range of platforms.

Available in both stand-alone and PC-connectible configurations, SecuGen has made it possible for SecuGen sensors to be integrated into nearly any type of application based on a variety of platforms in order to meet the specifications required by you or your clients.

Software applications can be developed for use with SecuGen peripherals on: Windows Server 2003, Windows XP, Windows 2000, Windows NT 4, Windows Me, Windows 98, Windows 95, Windows CE, Windows CE .NET, Linux, and DOS.

New Reason #6. SecuGen sensors are now better than ever

All SecuGen sensors in current products now feature second-generation optic modules that work even better with dry and difficult-to-use fingerprints, such as worn and aged skin, thanks to a higher signal-to-noise ratio compared to earlier modules and improvements to the performance of our algorithms.

A Comparison:

SecuGen's Optical vs. Capacitive (Semiconductor) Fingerprint Sensors

	SecuGen Sensors	Capacitive Sensors

Sensor Type	Optical (Patented SEIR method)	Capacitive (Semiconductor or chip)
Sensor Surface	No special treatments or maintenance required	Usually needs surface treatments, including ESD and other protective coatings Coatings may be uneven, wear out over time, degrade performance, and shorten product lifetime
Overall Durability	Scratch-proof, unbreakable glass platen made of material as hard as quartz Resistant to shock, ESD, and extreme weather	Corrodes easily from repeated handling and everyday exposure Susceptible to damage by electrostatic discharge Thin silicon chips are inherently fragile and susceptible to damage by hard external impact and scratches
Imaging Area, Resolution, and Size	Large imaging area (0.5 inch x 0.6 inch) High resolution (500 dpi) Large image size (78,000 pixels)	Usually smaller imaging area, image size, and resolution due to greater cost of manufacturing larger, high quality chips
Cost-Effectiveness	Low manufacturing cost, long life, no maintenance required	Consistent quality surface coatings may be expensive to produce Replacement, maintenance, and downtime costs can add up
Warranty	One year	Information not readily available