CDVI
Access Control Manufacturer

FingerPrint Reader DGID

(Wiegand Version 3.0)

for Windows (2000, XP)

User Manual
Sept. 2006

TABLE OF CONTENTS

USER MANUAL

DGID FINGER PRINT IDENTIFICATION SYSTEM

I. Overview

DGID SOFTWARE

Minimum System Requirement:

- Pentium CPU, 166MHz
- 32 MB of memory
- 3 MB of disk space for application, 5 MB of disk space during installation
- A Color Graphic-adapter (High Color (16 bit) at 800 x 600 Pixels)
- A floppy 3.5” disk drive
- Windows 95, 98, NT4.0 (SP 6) and Windows 2000

General features:

- Runs under all Windows platforms (95, 98, NT4.0, XP, ME and Windows 2000)
- Runs also on Windows-driven “slow computer” (486)
- Uses the same database-structure for databases on the device and on the host.
- Distinguishes between biometric and non-biometric devices, connected to COM-port of host.
- Determines automatically, which biometric device (EACM or DGID) is connected to a COM-port (COM1 to COM4).

DGID TECHNICAL SPECIFICATIONS

- Input Voltage 12VAC/DC. Current Consumption in rush: 150 mA
- Stores up to 1000 Fingerprints in the local database.
- 1 Relay output N/O & N/C contact 3A/125V and buzzer on board,
- 3 LED’s for indication of the sweeping direction for fingerprint recognition.
- 1 Request-to-Exit input
- 1xRS232 + 1xRS485,
- Option 26-bit wiegand Output
- Tamper Switch 0.5 Amp@50 V ~ or = N/C contact
- TCP/IP support on-request
- 2 MB Flash-Memory, 1 MB SDRAM, 32-bit Hyperstone DSP/RISC Processor with up to 220 MHz.
- High image quality and full-sized fingerprint image capture based on finger sweeping with 500 dpi resolution, 256 grayscales and 320 x 440 pixel
- Based on the thermal-electric CMOS sensor from Atmel
- Finger auto detection
- Self cleaning sensing area (auto cleaning)
- Operation temperature: -30 to +70 Celsius
- Naturally protected against ESD: > 16 kV air discharge
- Resistant to abrasion: > 1 million finger sweeps

- Drivers for Microsoft Windows 98/ME/2000/XP
- Encrypted communication link with the PC
- Support of a dynamic firmware-upload respectively firmware-update

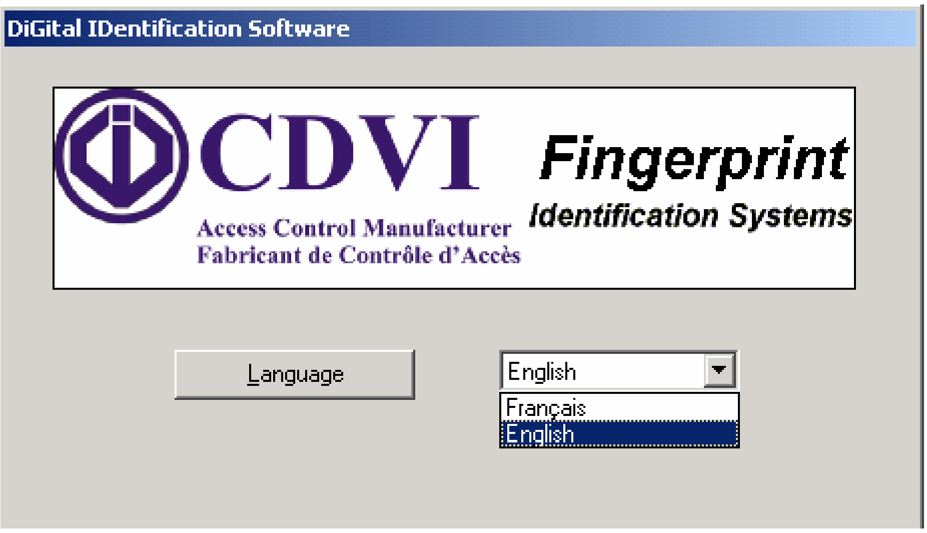
II. INSTALLATION (Hardware and Software)

1. -Connect your device to host (on any available COM-port) and ensure that device is correctly connected and powered on. System will automatically find out the Finger print reader is connected to the COM-port.
2. -Close all other Windows applications, before you start with installation of the DGID Finger print software.
Run setup located on the root of the Floppy 1 of 2. It is recommended to accept all default setting.
At the end of Setup-routine you will be asked to reboot the Installation-PC. (Recommended, so that all DLLs get a chance to register themselves into system registry).
3. -Start the DGID software on your desktop. Automatic firmware upload and device database deletion might appear if necessary. The "Control-Panel" of the software appears. You may start **"Training"** to check the availability of the "Application-System".

Note:
The transfer of a (high resolution) fingerprint image (with a size of up to 200 Kbytes) via a slow communication-link (RS232, max. speed 10 Kbytes/s) takes time. Therefore image is highly compressed before sending it to host. Displaying of compressed image on the host is only for your monitoring purpose. Biometrics process of image is performed in the device before compression. Device driver constantly acknowledges each received data-package from the device, so that maximum security is also obtained.

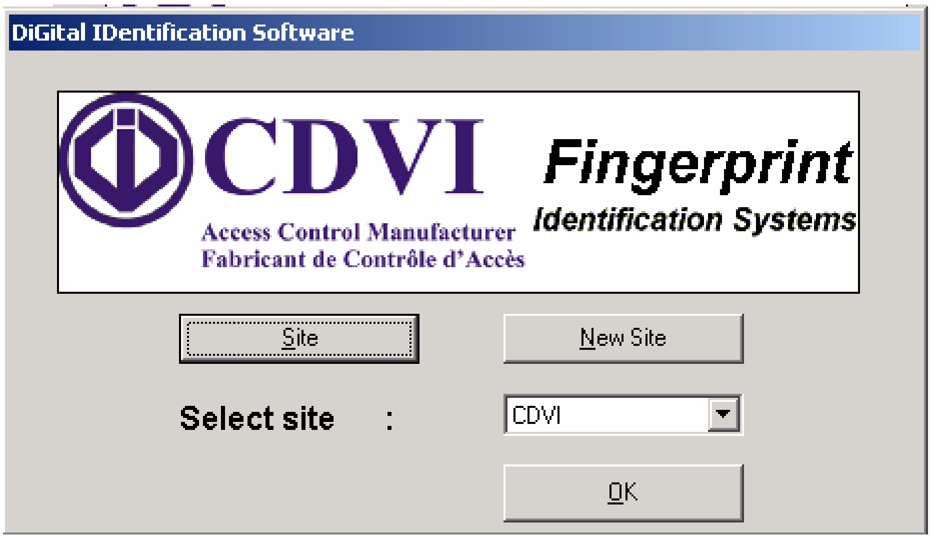
III. SELECT LANGUAGE

To select a language click on the drop list and then click on the icon "Language" to confirm.


DiGital IDentification Software
CDVI
Access Control Manufacturer
Fabricant de Contrôle d'Accès
Fingerprint
Identification Systems
Language
English
Français
English

IV. SELECT A SITE

The DGID multiple-site software allows to manage and to control more than one Finger print reader with the same software. If the site exists already choose the name in the site directory or click on the icon "New Site" to create one. It will save the data of the new site in a separate directory:

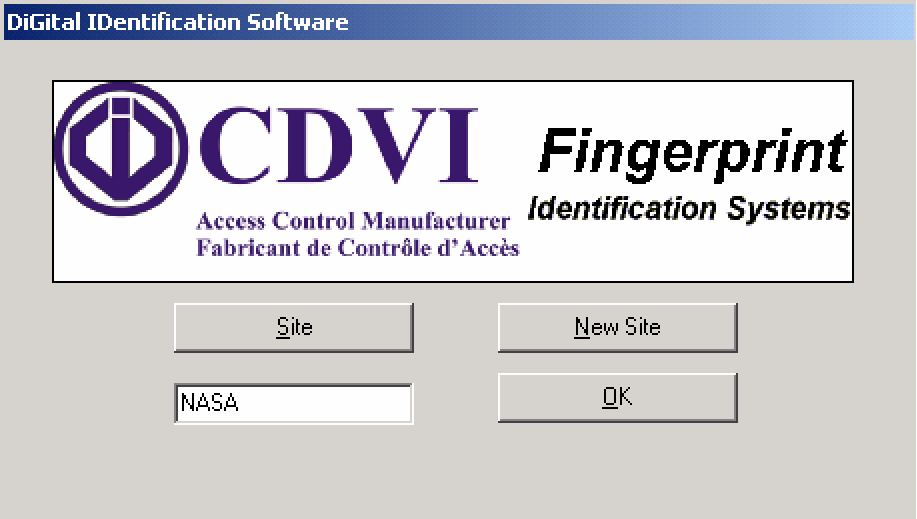

DiGital IDentification Software
CDVI
Access Control Manufacturer
Fabricant de Contrôle d'Accès
Fingerprint
Identification Systems
Site
New Site

Select site : CDVI

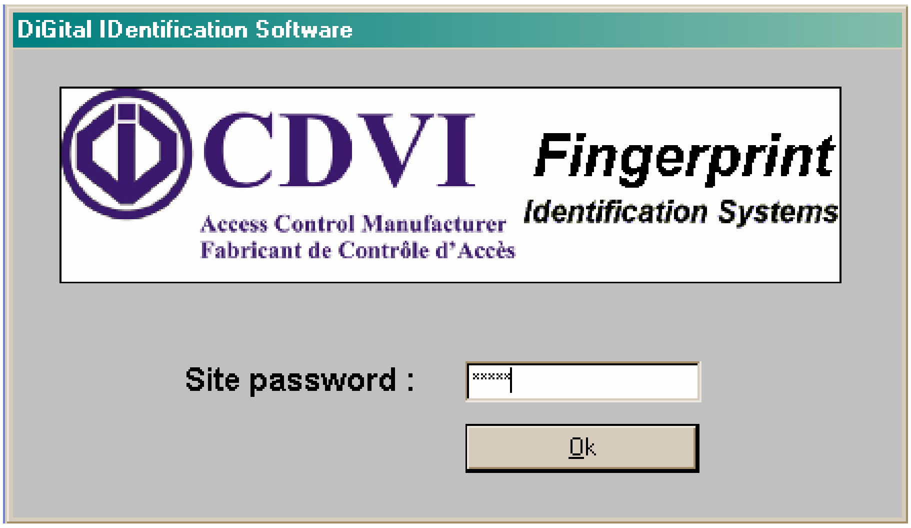
If the site exists click on the drop list icon to display the site list and select in one site name:

Once the site has been selected click on the “OK ” button.

For a new site enter the name of the site in the blank space. To save the new site press on “ Enter ” or click on the “ OK ” button:


DiGital IDentification Software
CDVI
Access Control Manufacturer
Fabricant de Contrôle d'Accès
Fingerprint
Identification Systems
Site
New Site

NASA

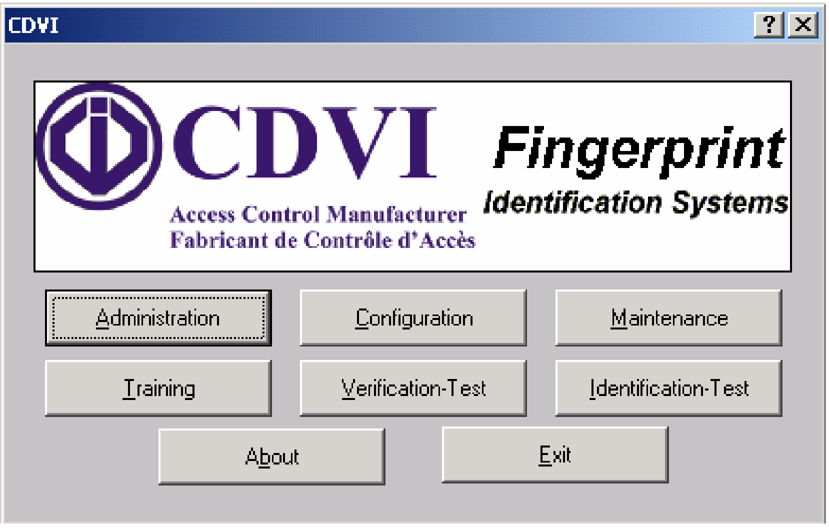

DiGital IDentification Software
CDVI
Access Control Manufacturer
Fabricant de Contrôle d'Accès
Fingerprint
Identification Systems

Site password : *****

Enter the Password and click the OK icon (12345 Factory default Value).

V. CONTROL PANEL

The DGID software consists of 6 software modules: “Administration”, “Configuration”, “Maintenance”, “Training”, “Verification-Test” and “Identification-Test”.



The DGID and EACM Systems operate in 2 different operation modes: AS-mode and FS-mode. This enables you to use Embedded Biometric Systems in stand-alone and network Environments.

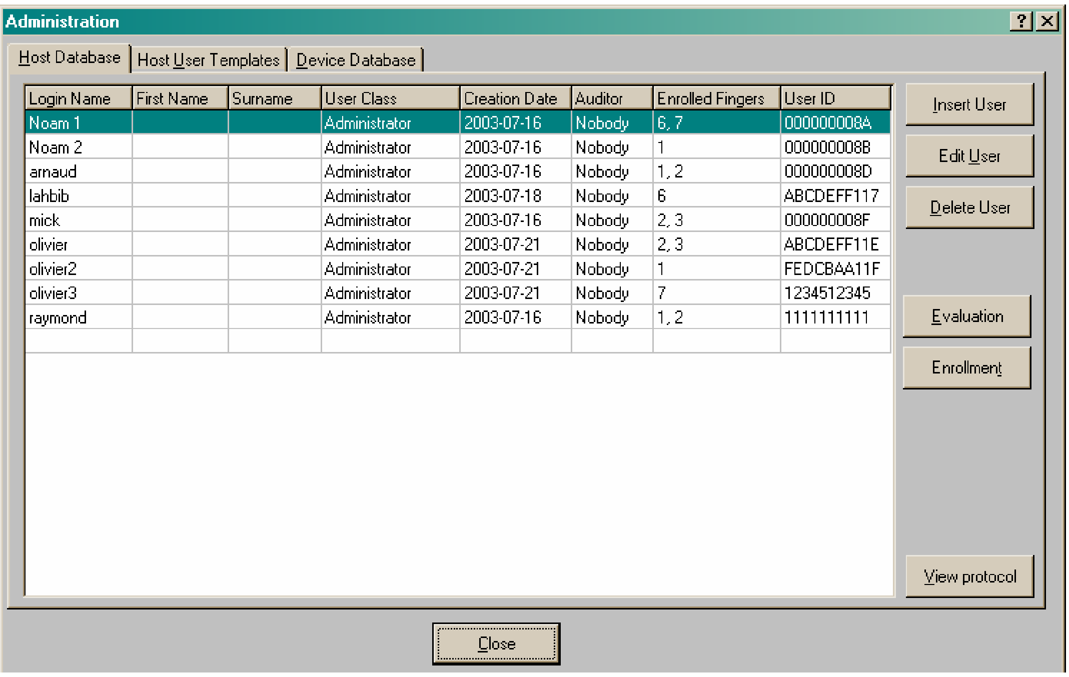
Authentication Subsystem-mode (AS-mode):

In this mode “Device” provides complete functionality of fingerprint biometrics. The database will be located (activated) in device . Only an encrypted signal for successful verification / identification is returned.

Fingerprint Code Supplier- mode (FS- mode):

In this mode fingerprint biometric functionality are shared between “device” and the “host”. Device captures the fingerprint and extracts the biometric data. It delivers an encrypted Fingerprint Code (FP-code) to the host. The (local or remote) host manages the templates and performs the verification / identification. The database will be located (activated) on the host.

A. ADMINISTRATION



Login Name	First Name	Surname	User Class	Creation Date	Auditor	Enrolled Fingers	User ID
Noam 1			Administrator	2003-07-16	Nobody	6, 7	000000008A
Noam 2			Administrator	2003-07-16	Nobody	1	000000008B
arnaud			Administrator	2003-07-16	Nobody	1, 2	000000008D
lahbib			Administrator	2003-07-18	Nobody	6	ABCDEFF117
mick			Administrator	2003-07-16	Nobody	2, 3	000000008F
olivier			Administrator	2003-07-21	Nobody	2, 3	ABCDEFF11E
olivier2			Administrator	2003-07-21	Nobody	1	FEDCBAA11F
olivier3			Administrator	2003-07-21	Nobody	7	1234512345
raymond			Administrator	2003-07-16	Nobody	1, 2	1111111111

The Administration module is used for user enrollment and management (at host and device-level).

Short description of some buttons:

The button "Host Database":
Shows the inserted user (with or without enrolled fingers into Host Database.
· **Login Name:** A unique string in Host Database.
· **Registration Date:** The date of inserting the user was to the Host Database,
· **User:** First name and Last name
· **User Class:** See "Insert User"
· **Enrolled Fingers:** Displays which finger(s) of a user is (are) already enrolled.
. **User ID :** Displays the ID which is associated to user fingers.

The Button "Host User Template"
Shows templates of selected user, residing on the "Host Database". You can choose one (or more, not yet implemented) template to remove it from Host Database or upload it (including related user-information) into "Device Database".

The Button "Device Database":
Shows the registered user templates in the device. You can delete a selected record (Template of the enrolled finger with related user-information) from database of the device. Click on the button **"Delete"** the selected record or to delete all records click on the button "**Delete all**". Click on the button download to download the **"Device database"** to the **"Host Database".**
The occupied flash memory through user-information are visually displayed.

The button Enrollment:
· First you insert a new user to the database. The new user will be inserted **ONLY** into the Host Database.
· You select the inserted user and press on the button "**Enrollment"** to enroll one (or more) finger of the selected user.
You can also first click on the button "**Evaluation"** to determine, which finger of a user is (are) best suitable for creation of (reference-) template and then immediately enroll the (by system) proposed fingers.

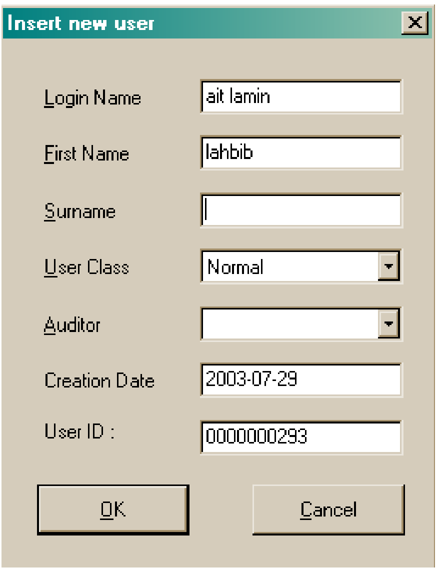
Biometric Device operating in AS-mode: (host-independent)

· To let device operates in the AS-mode, it is needed that at least one user with at least one enrolled finger is stored in the "Device Database". Otherwise the LED will remain off, when you exit
the DGID software or disconnect the device from the host.
· You exit the software or disconnect the biometric device from host (but power is needed!) to identify (1:n-matching) registered user fully host-independent.

LED functionally of device operating in AS-mode:
a) DGID Finger Print reader:
3 LED flashes (green) one after the other Standby mode (Waiting for Scanning finger)
LED flashes (green) slowly (first LED from the bottom) User can not be identified
LED flashes fast for a few seconds (green) Quality of finger is too low
LED lights for a few seconds (green) and a beep is emitted User is identified
b) EACM:
LED lights constantly Standby mode (Waiting for Scanning finger)
LED lights for a few seconds constantly, also the LED
connected to the "Relay Control Port" of EACM (green) User is identified
LED lights a few seconds constantly (red) User can not be identified

1. Insert User

Click on the button “Insert User” to create a new User:



Login Name: ait lamin

First Name: lahbib

Surname:

User Class: Normal

Auditor:

Creation Date: 2003-07-29

User ID : 0000000293

Login Name:
A string used at verification-time. Login Name is unique in the Host Database and has to be entered in the maximum size of 20 characters. Note that Login Name is **case sensitive.** It can be the same as the First Name of registered user.

Note:

· Login Name field can’t be left empty. The database is checked to avoid duplicate of Login Names.

· Registration Field will be filled out automatically with actual “System-Date” of host and can not be changed.

User Class:

Controlled: A user, who is under control of Auditor(s).

Auditor: A user, who controls the other user(s). This user can be also a normal user.

Administrator: A user, who has the right to perform tasks for user management, configuration and
maintenance of device.

Normal: A user with no User Class of Admin, Controlled or Auditor.

Normal (Auditor): Normal user that also has right to control Controlled users.

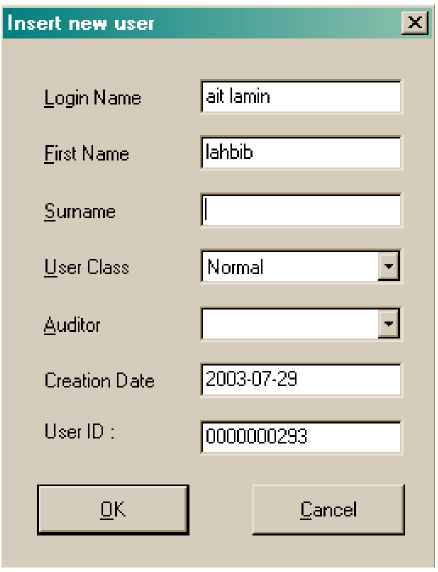
Administrator (Auditor): Administrator, who that also has right to control Controlled users.

USER ID: code generated automatically by the software for each user and to be used for the UGL/UGM access control systems (refer to Badge in the LOG/MTSE software). The code can be set in decimal or hexadecimal from the Configuration menu.

Note: Only the user class “Normal” is supported in this version. However you can enter users with different users class for usage in next version.

2. Edit User

Change of most user information can be done here.



Login Name: ait lamin
First Name: lahbib
Surname:
User Class: Normal
Auditor:
Creation Date: 2003-07-29
User ID : 0000000293

Note: You can not change the fields Login Name and Creation Date.

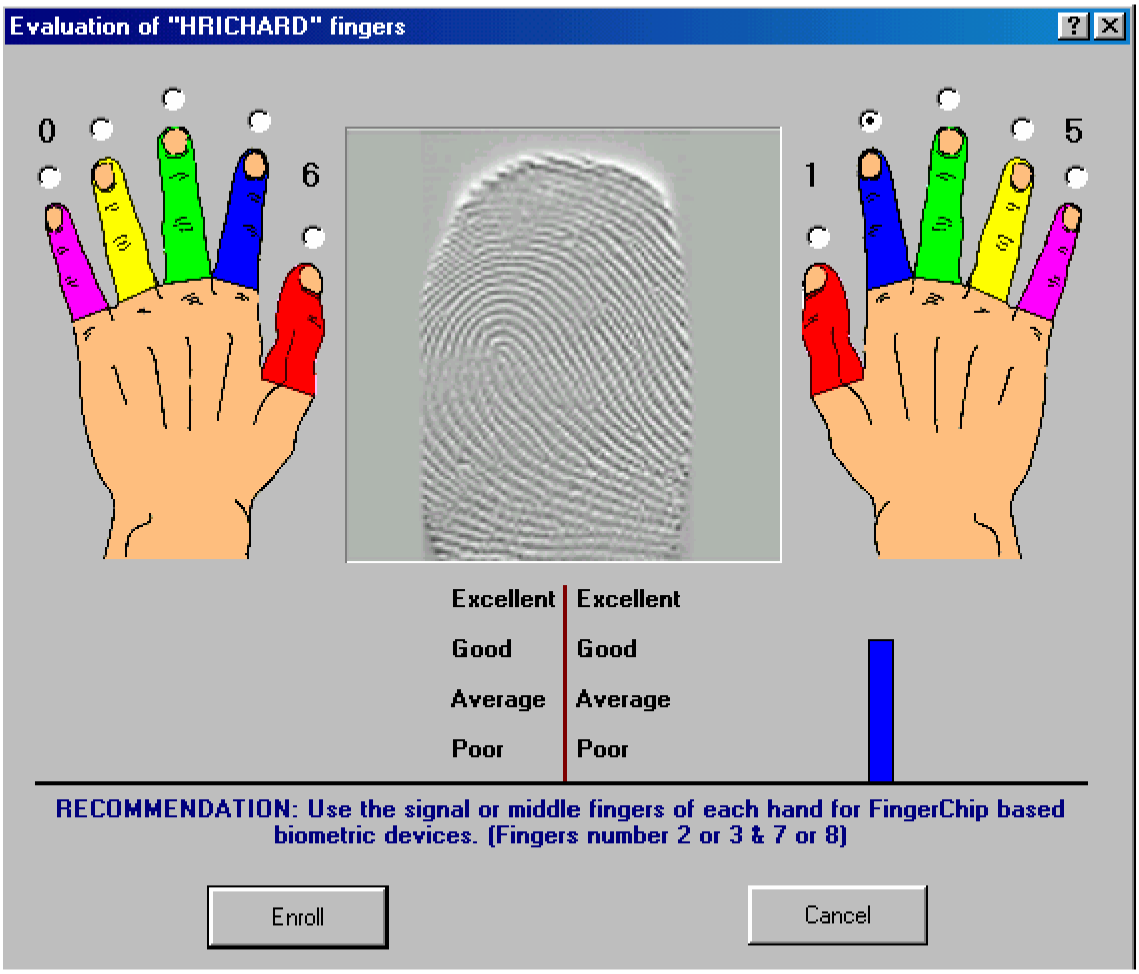
3. Delete User

The user can be deleted from the Host Database. Select the user to delete and then click on the Delete icon then a warning message is displayed to confirm the deletion. Press OK to delete the User.

The user can be deleted from the Device Database. Select the user to delete and then click on the Delete icon then a warning message is displayed to confirm the deletion. Press OK to delete the User.

4. Evaluation

You can also first click on the button "**Evaluation"** to determine, which finger of a selected user is (are) best suitable for creation of (reference-) template and then enroll the proposed fingers by the system.



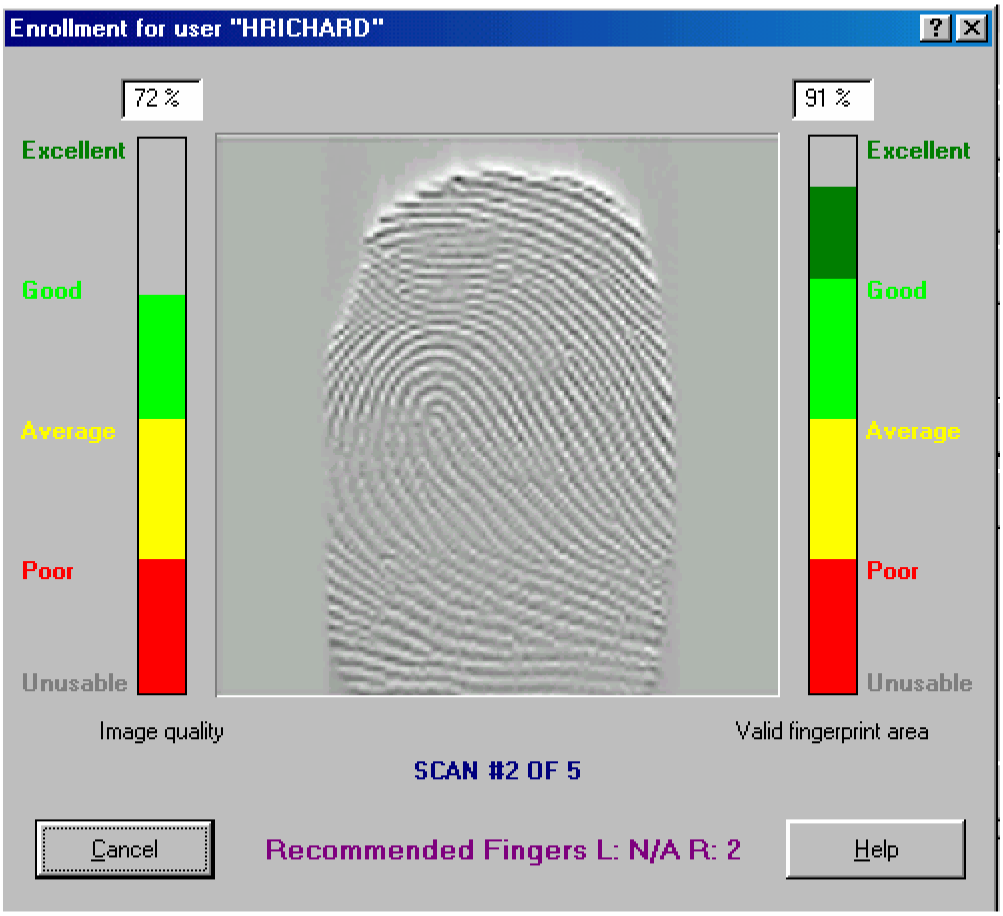
Evaluation of "HRICHARD" fingers

RECOMMENDATION: Use the signal or middle fingers of each hand for FingerChip based biometric devices. (Fingers number 2 or 3 & 7 or 8)

· Click on the finger, capture fingerprint and evaluate it.
· The names and number(s) of proposed finger(s) will be displayed in status-filed of enrollment's window (the next upcoming window, after click on "Enroll"-button).
· You can skip the evaluation of user's fingerprints too. (just click on the button "Enroll")

5. Enrollment

For the enrollment of a new user one or more templates must be created for storage in the Host Database. Each template will be created from a number of fingerprints of the same finger. That number is adjustable, conveniently it lies in the range from 3 to 10. The default number of 5 is recommended for most cases. After "n" accepted fingerprint-images the following Window appears: (setting template-parameters)



Enrollment for user "HRICHARD"

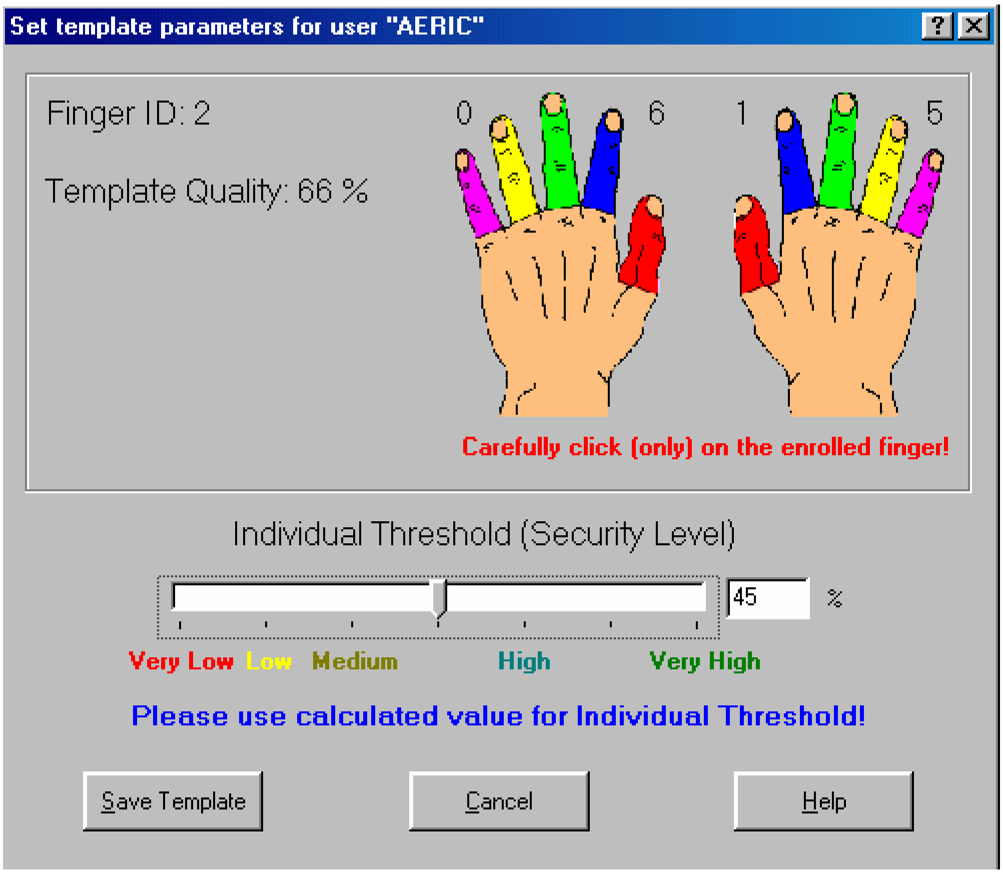
Image quality: 72 %

Valid fingerprint area: 91 %

SCAN #2 OF 5

Recommended Fingers L: N/A R: 2

Finger-ID: The number of enrolled finger. You have to click (carefully) on the enrolled finger.
Template Quality: The template quality value is scaled within a range from 0 to 100 and has the unit percent. 100% means the highest possible quality. Template Quality is calculated internally by the algorithm.
Individual Threshold: (Security Level for Verification 1: 1 matching)
The biometric capability varies from fingerprint to fingerprint. Hence, an individual threshold is added to each template to reach an optimal system performance. By default, the individual threshold is used in verification mode matching. During enrollment, a proposal for the individual threshold is calculated. It is recommended to accept this value or you may (carefully) change it.



Set template parameters for user "AERIC"

Finger ID: 2

Template Quality: 66 %

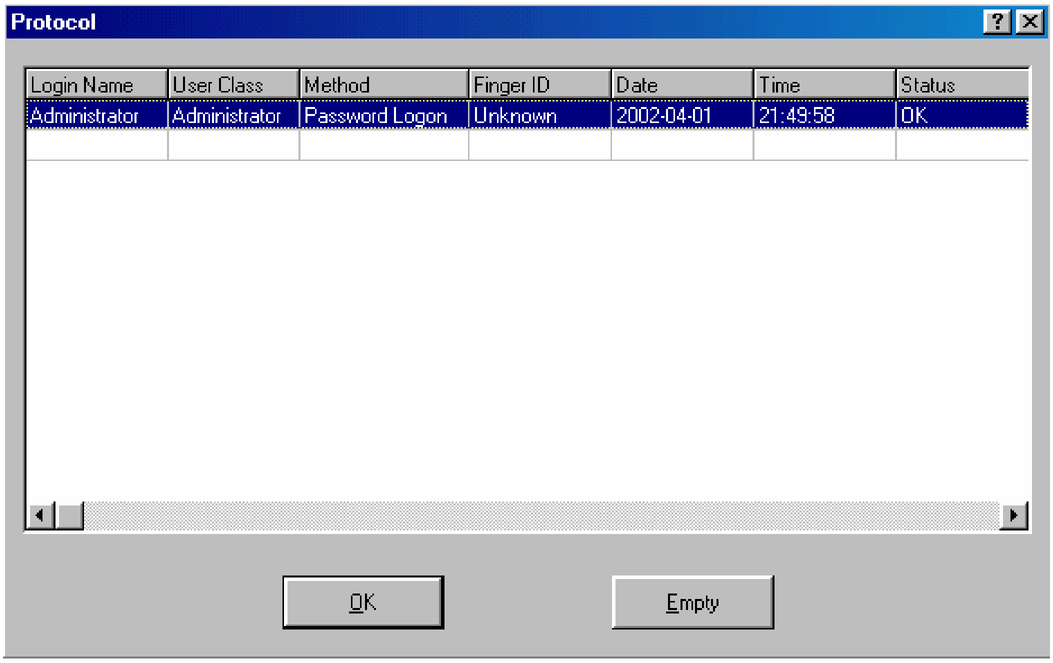
0
6
1
5
Carefully click (only) on the enrolled finger!
Individual Threshold (Security Level)
45
%
Very Low
Low
Medium
High
Very High

Please use calculated value for Individual Threshold!

Save Template
Cancel
Help

Click on the button “Save Template” template and it’s set parameters will be stored in the Host Database. After finished enrollment of a finger you will back to “Administration Window”. You can enroll other fingers for this user.
Once the Template has been saved in the Host Database then it must be uploaded in the Device Database. Select the user in the Host Database list and click on the Host User Template button. All templates from the user will be displayed, select one template and click on the icon Upload. The template is then transferred to the Devise Database.

6. View Protocol

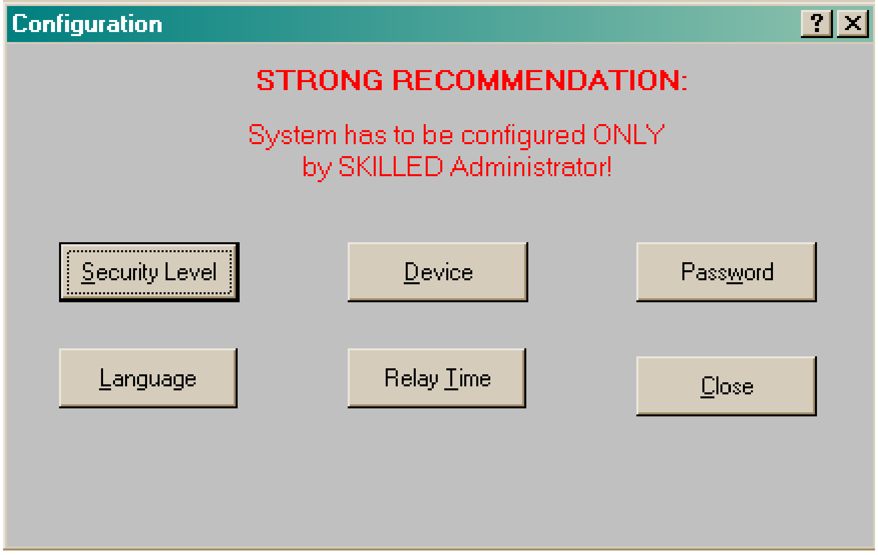


Protocol

Login Name	User Class	Method	Finger ID	Date	Time	Status
Administrator	Administrator	Password Logon	Unknown	2002-04-01	21:49:58	OK

Displays the result of identification or verification processes for all users.

B. Configuration



Configuration

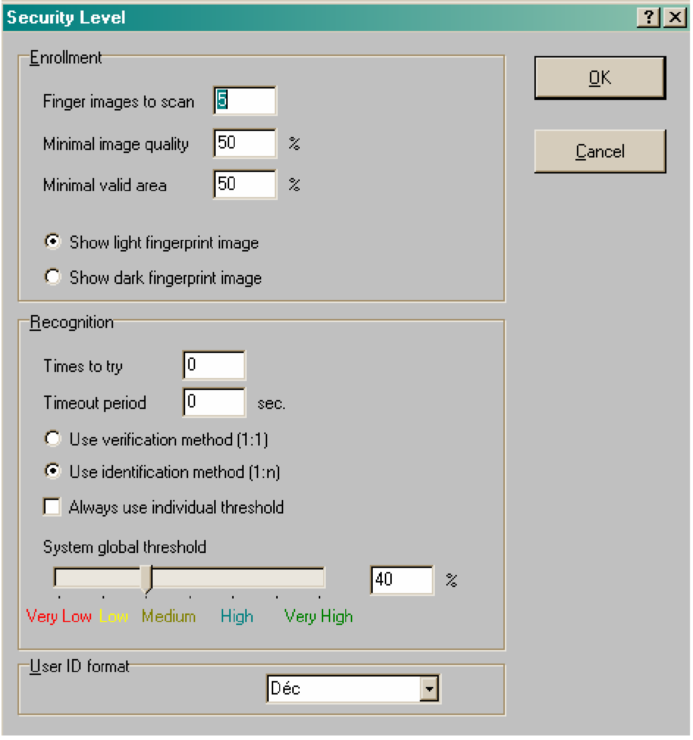
STRONG RECOMMENDATION:

System has to be configured ONLY
by SKILLED Administrator!

Guard: Setting up system security (software and hardware)
Language: Choose another language. Currently French and English languages are supported.
Device: Get device configuration.

1. Security

a) Enrollment



Security Level

Enrollment

Finger images to scan: 5

Minimal image quality: 50 %

Minimal valid area: 50 %

● Show light fingerprint image

○ Show dark fingerprint image

Recognition

Times to try: 0

Timeout period: 0 sec.

○ Use verification method (1:1)

● Use identification method (1:n)

□ Always use individual threshold

System global threshold: 40 %

User ID format: Déc

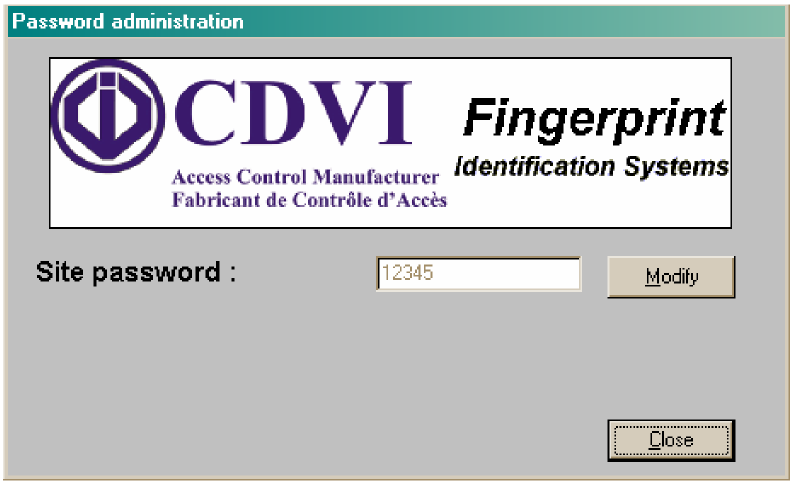
Finger image to scan:
The quantity of accepted fingerprint-images (of the same finger) for creating a template.
Minimum Image Quality:
Minimum Image Quality of captured fingerprints during enrollment. Fingerprints with quality less than this value will be rejected.
Minimum valid area:

Minimum useable area of captured fingerprints during enrollment. Fingerprints with quality less than this value will be rejected.
"Show light fingerprint image" "Show dark fingerprint image":
How to display the captured fingerprints on the host-screen
User ID format : allows to create User ID in Hexadecimal or in decimal.

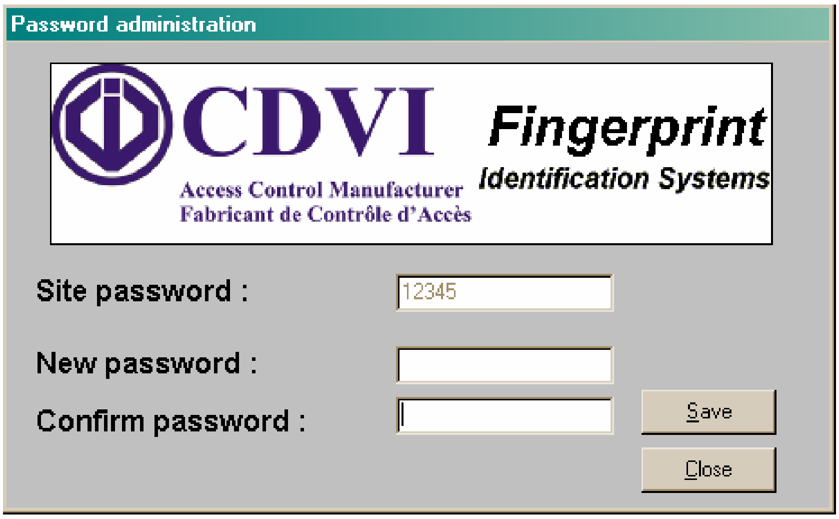
b) Recognition

Times to try: (Not supported in this version.)
0 means no limitation.
It determines how often a user can try to be identified or verified. (Default setting = 3)
Timeout Period: (Not supported in this version.)
0 means no limitation.
Use verification method (1:1) Use identification method (1:n): (Not supported in this version)
These parameter are used for identification or verification of user, who are allowed as administrator to manage and configure the system.
"Always use the individual threshold" and "System global threshed"
The DGID software distinguishes between individual and global thresholds.
The value of individual threshold depends on template quality. The DGID software determines and proposes this value during enrollment of finger. The Admin has also the opportunity to adjust it fine. The set value of individual threshold will be stored in any template. The DGID software sets also a default value for global threshold, which can be adjusted with care by a skilled person.
By default 'Global Threshold' determines the security-level in identification mode. A high set value gives a higher security-level but also the False Rejection Rate increases (FRR)!
Admin can change the default behavior of identification process by changing the default setting of the above mentioned DGID software-parameter.
Adjustable global and individual thresholds and proper settings of related parameters enables the "Application-System" to handle fingerprints with regards to their quality.

2. Password



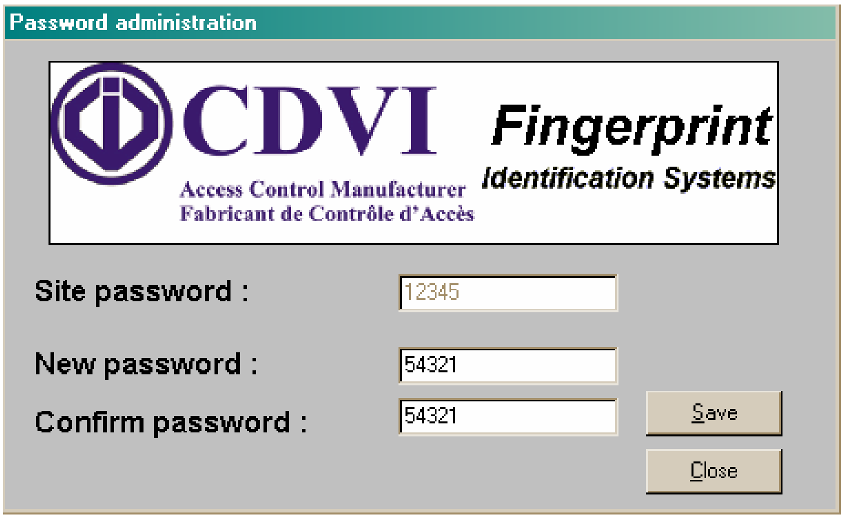
Site password : 12345



Site password : 12345

New password :

Confirm password :



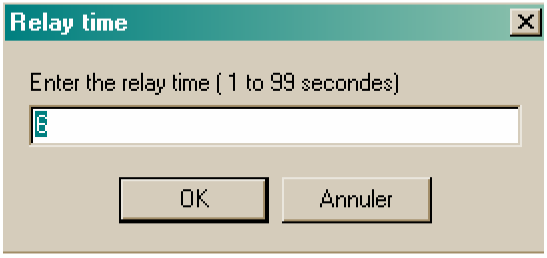
Site password : 12345

New password : 54321

Confirm password : 54321

To change the password click on Modify icon. Enter the new password and then enter the password to confirm. Click on Save. To go back to the main menu click on Menu.

3. Door Release Time



Enter the relay time (1 to 99 secondes)

6

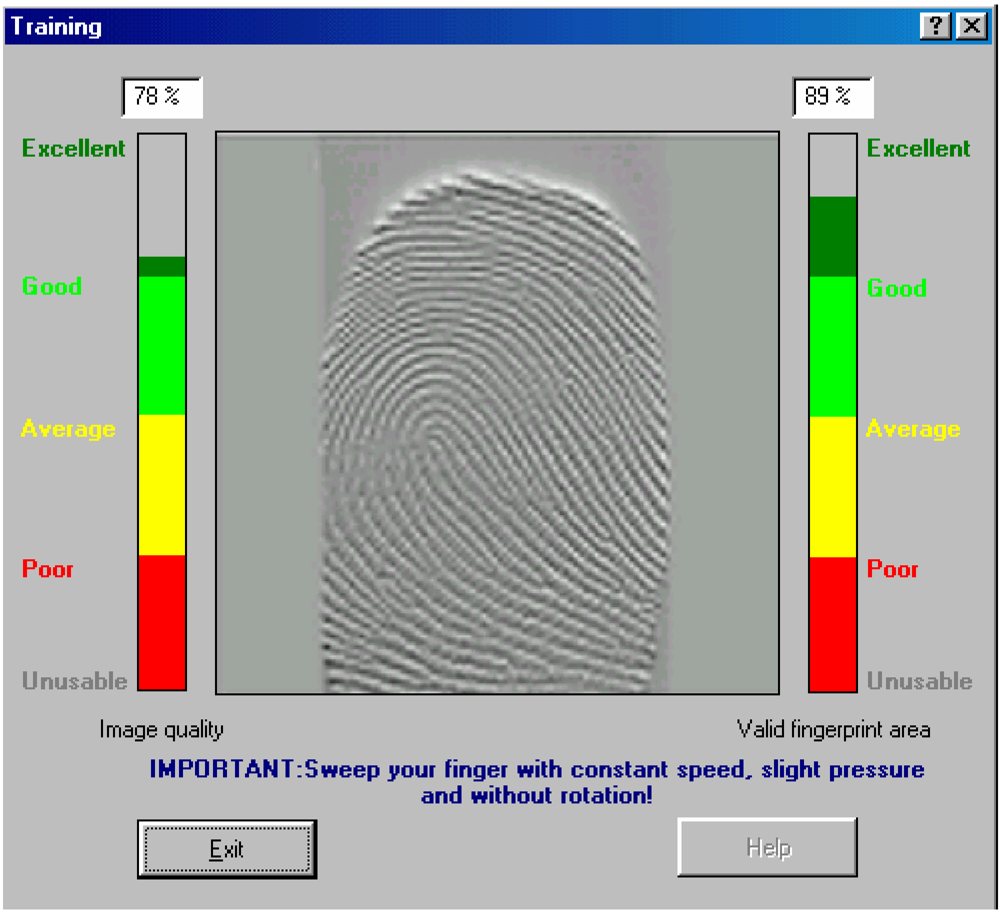
To set another time click on the Relay time icon and then enter the new door release time and click on OK to confirm. Click on the Menu icon to go back to the main menu

C. MAINTENANCE

For the Factory Use Only
A utility for update of firmware

D. TRAINING

The visual display of determined image quality and valid fingerprint area (area of fingerprint, which is useable for the DGID reader) assists the unskilled user to learn how to capture fingerprints with high quality.



IMPORTANT:Sweep your finger with constant speed, slight pressure and without rotation!

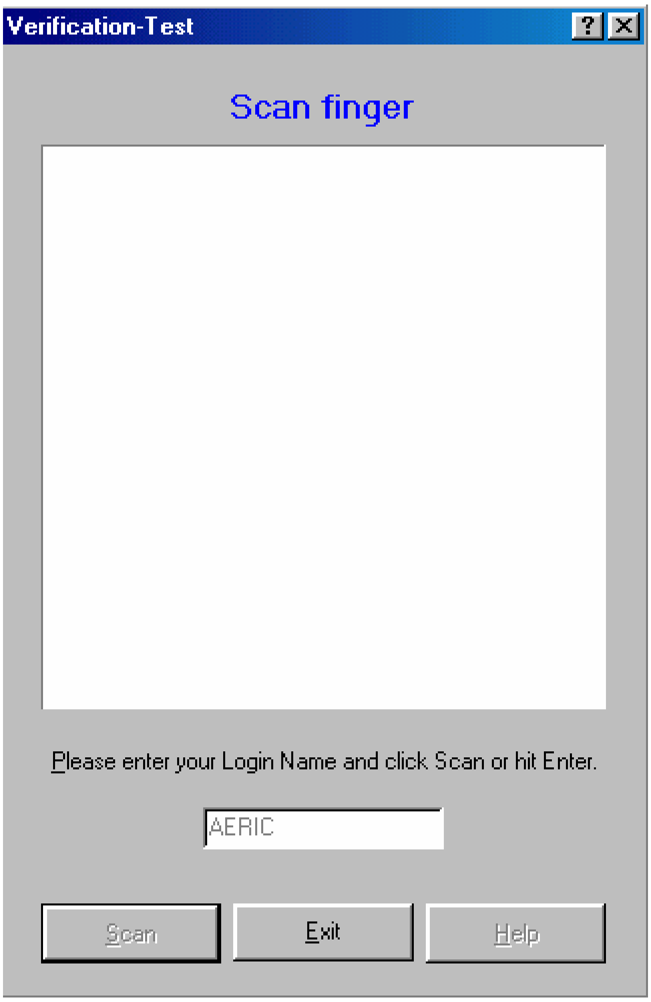
This module is multi-thread and therefore user-friendly. It means user captures fingerprints again without the need for further actions, like pressing a key or uses a mouse-button.
When you click on the button “Training” the LED of device:
· For EACM lights constantly (amber)
· For the DGID 3 LED’s flashes (green). One after the other showing the direction, in which the finger have to be scanned.

Note: Scan your finger as mentioned on the screen. If you can not see captured fingerprint on the screen, then something is wrong. Perhaps the device can not communicate with host. Check the physical connection and make sure that the DGID reader is powered.

E. VERIFICATION-TEST

The principle of verification is one to one.
The user first types in his/her “Login Name”. The DGID software distinguishes between small and capital letters. Then press on Enter or click on the button “Scan” and then scan your finger.
The message “Positive verification” appears, if user is verified.
The message “Verification failed” appears, if user can not be verified.

Note: For a new verification process, you have to enter your Login Name, press Enter or on the Scan button and capture a fingerprint.



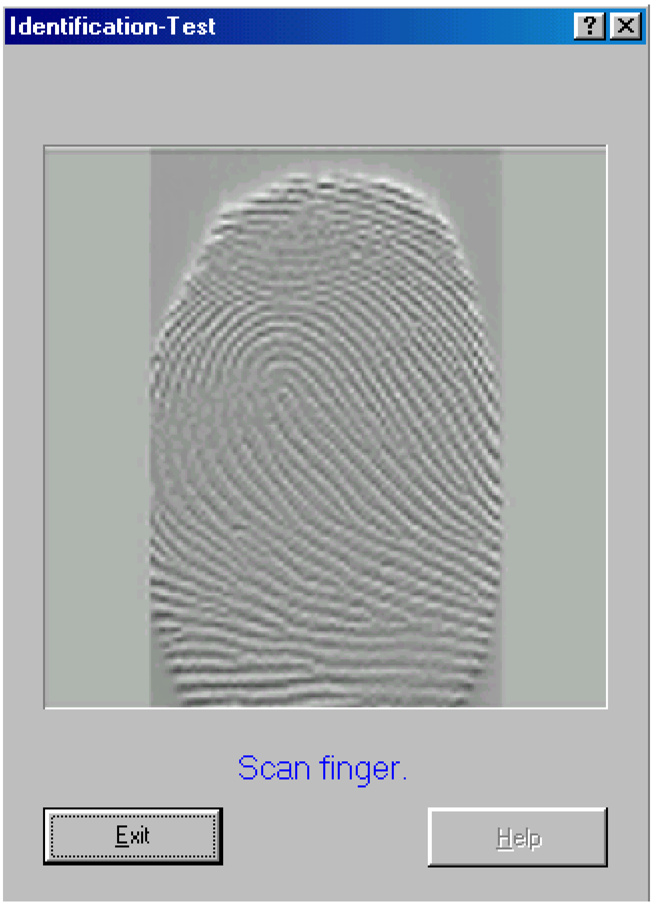
Please enter your Login Name and click Scan or hit Enter.

AERIC

F. IDENTIFICATION-TEST

The principle of identification is one to many. The user has only to scan his (her) finger over the FingerChip sensor.
The message "Welcome User Login Name" appears, if user is identified. Otherwise appears the message " Negative Identification".

Note: For a new identification process, simply scan your finger again.
Note: Identification-Test and Verification-Test are based on **FS-mode (**Finger Code Supplier) used By the DGID Embedded Biometric Device.
In **FS-mode** the biometric device, reads frames, reconstructs them to a whole image, creates Fingerprint Code, encrypts and sends it (including a compressed image of captured fingerprint) to the
host. The host decompresses the fingerprint image and displays it on the host-screen. The host matches (compares) the Finger Code with the template stored in the host database using "Global Threshold" (set by default 40%) or individual threshold based on system-settings.
Note: the DGID reader distinguishes between Finger Code and template.
In **AS-mode (**Authentication Subsystems) the device performs all above mentioned functionality including matching.
In the current version of the DGID software, the device is operationally in AS-mode, if it is (correctly) powered on and if the DGID software is closed (or device is disconnected form the COM-Port).



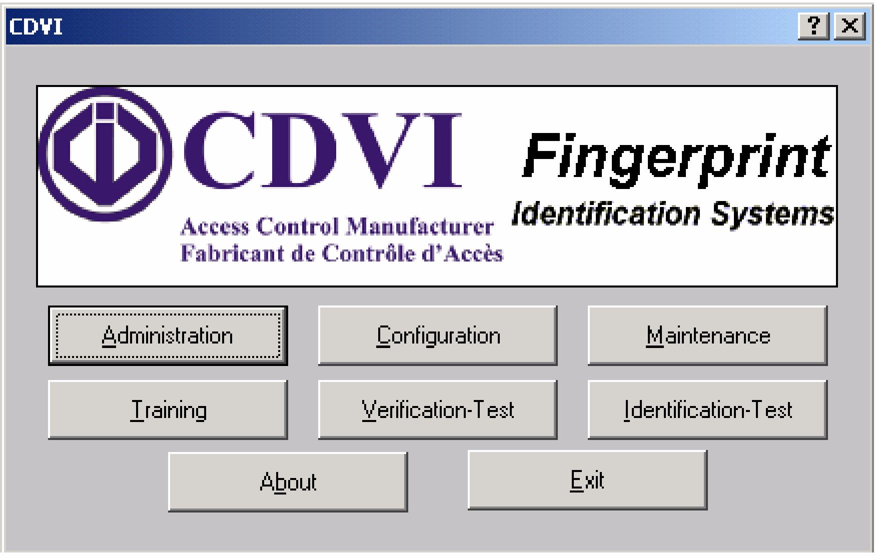
Scan finger.

VI. Network Setup

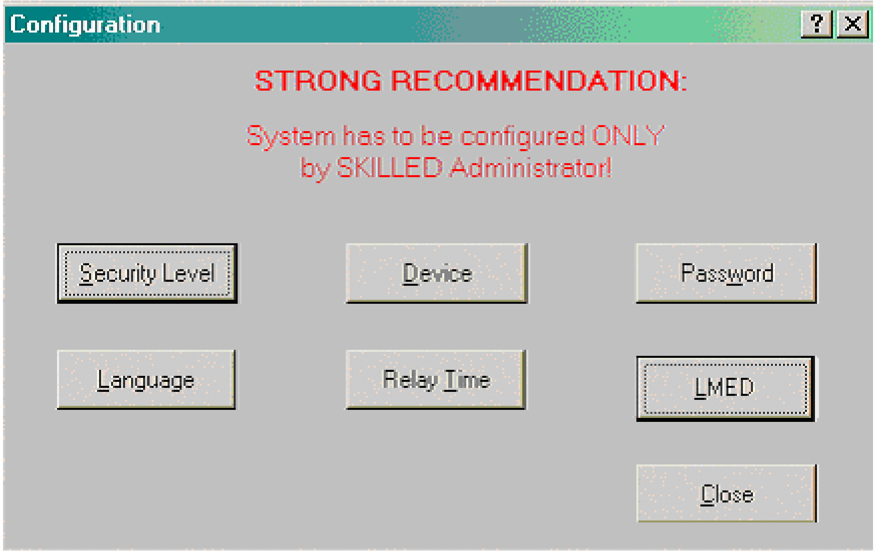
A. Software Configuration

The ES Manager software must be configured to start the communication between the software and the each device.

Once the software has been installed then connect the DGID RS232 to the PC.
In the main menu click on **Configuration**.



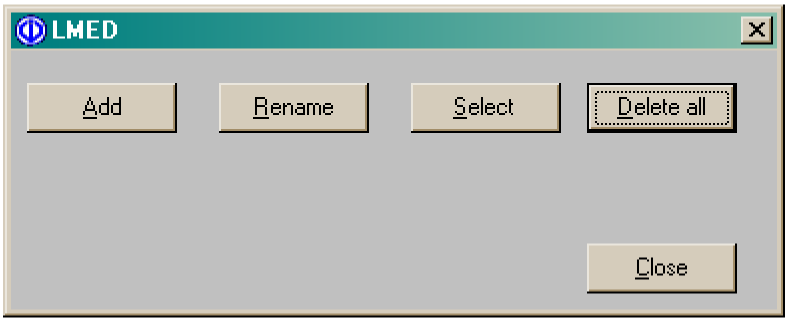
The configuration menu appears:



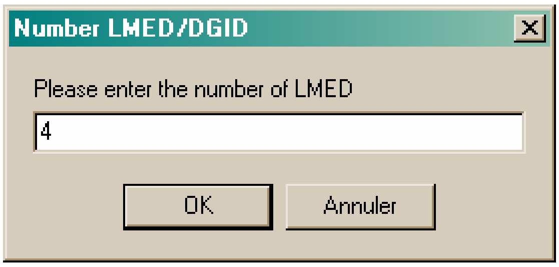
STRONG RECOMMENDATION:

System has to be configured ONLY by SKILLED Administrator!

Click on the LMED icon to enter in the setup menu:



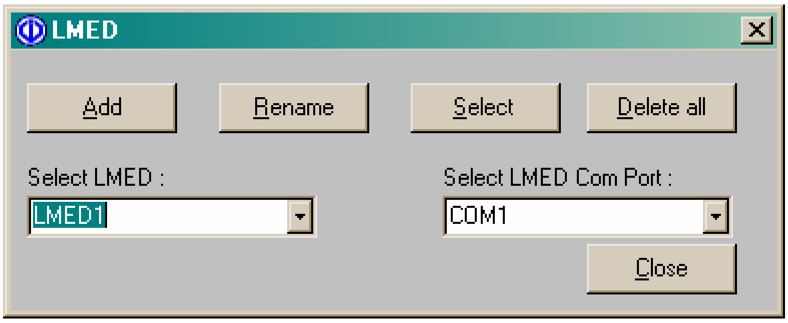
Add: Allows you to enter the number of DGID readers on the network. The quantity can be modified at any time.



Please enter the number of LMED: 4

Example: 4 DGID on the network

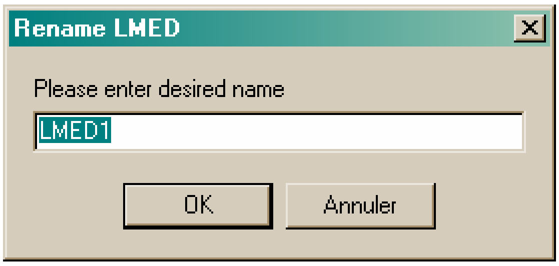
After entering the number of DGID unit, the DGID are created automatically as follow. LMED1 corresponds to the DGID with address 1, LMED2 corresponds to DGID with address 2.



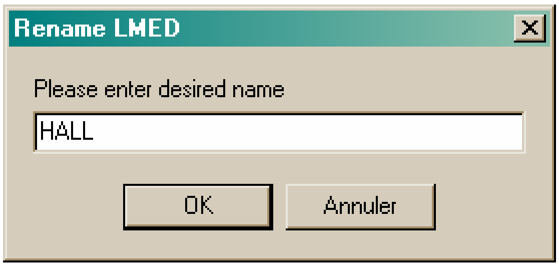
Select LMED : LMED1

Select LMED Com Port : COM1

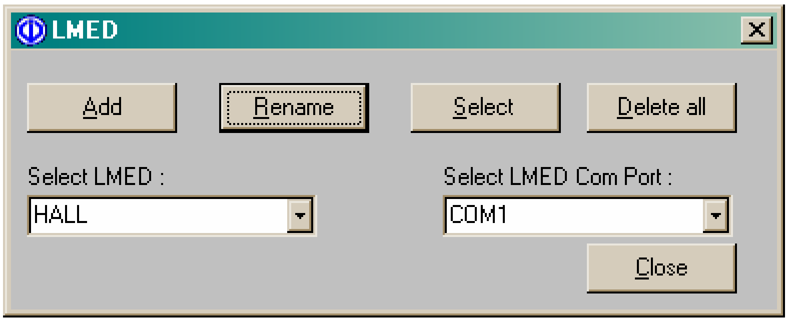
Rename: Click on the icon Rename to modify the name of a device.



Please enter desired name: LMED1



Please enter desired name: HALL



Select LMED : HALL

Select LMED Com Port : COM1

Select: Allows to establish a communication with the DGID selected in the list.

Delete: Allows to remove the DGID from the PC.

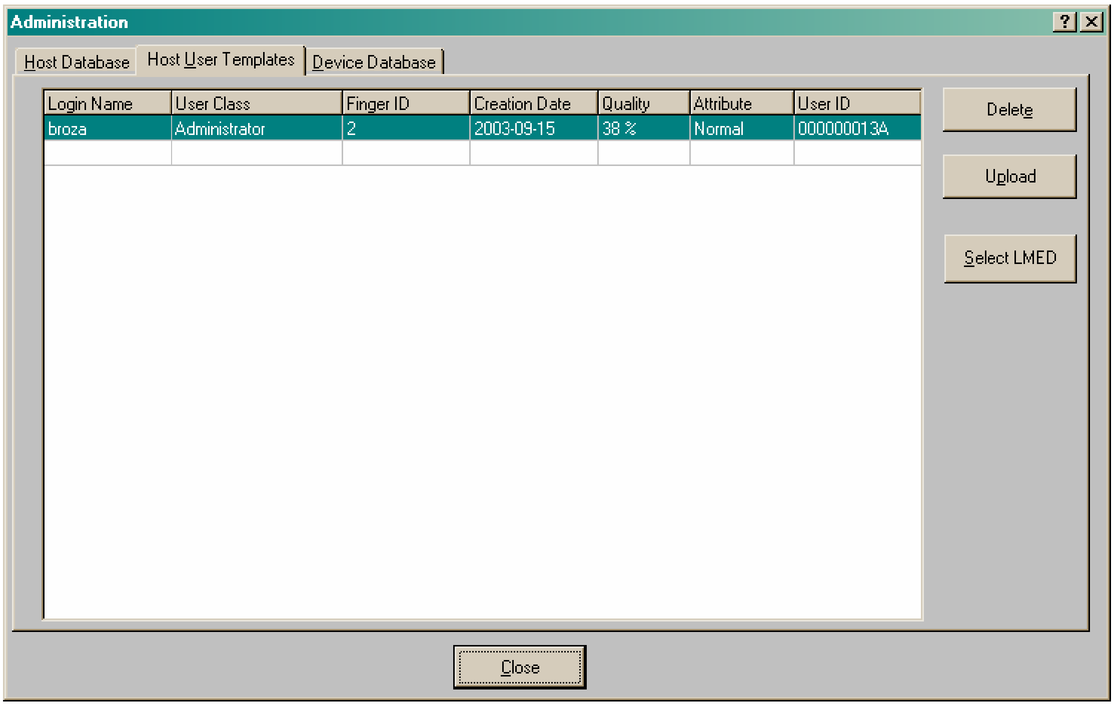
Comm. Port: Allows to select a comm. port.

Once the DGID devices have been set in the configuration Menu, then it is possible to get in communication with the LMED/DGID which are networked.

After entering the site password select the DGID device to which you wish to connect.

B. Select DGID

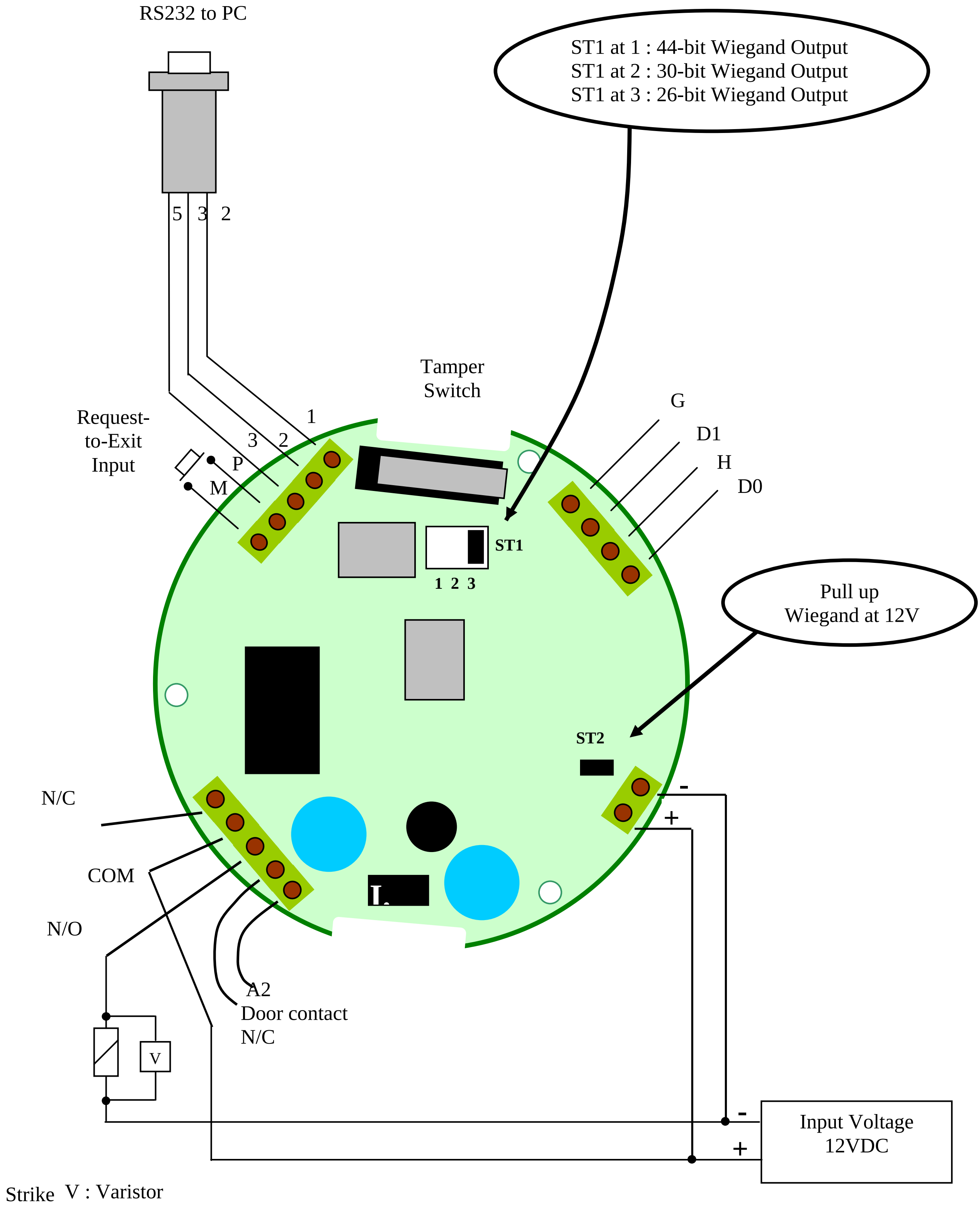
It is possible to select another DGID device while in connection with another device. Click on **Administration** icon then click on “Host User Template”.



Login Name	User Class	Finger ID	Creation Date	Quality	Attribute	User ID
broza	Administrator	2	2003-09-15	38 %	Normal	000000013A

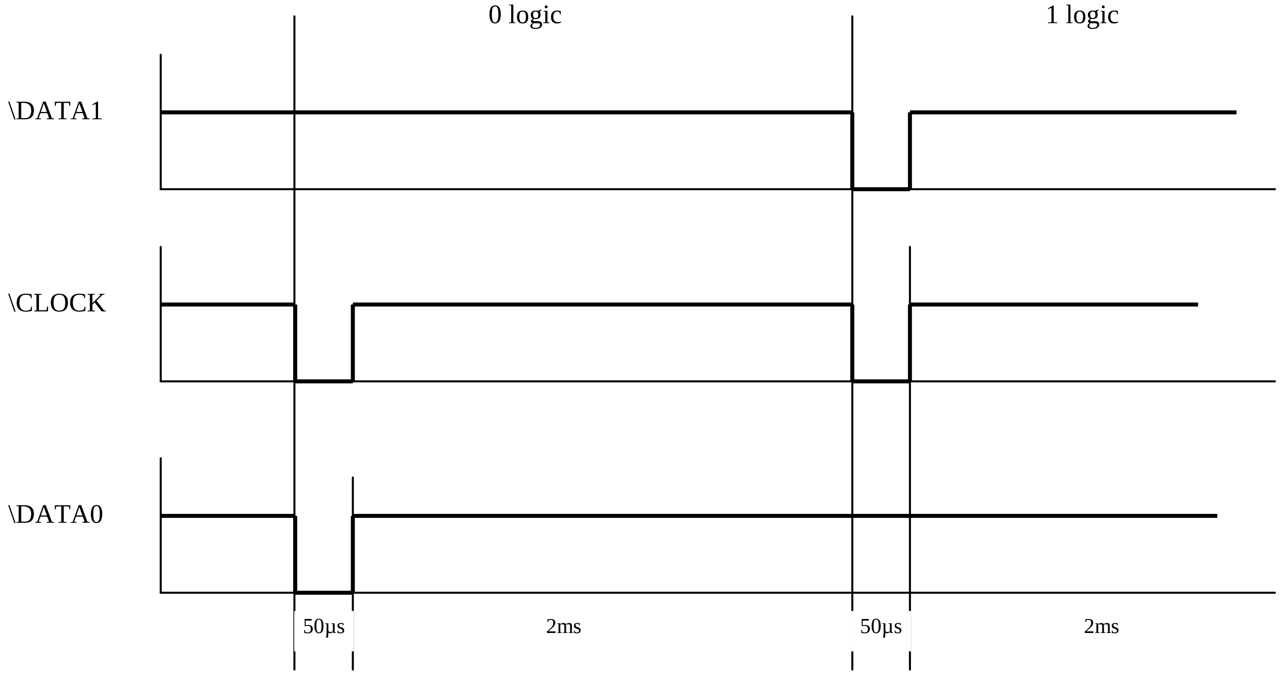
Click on the icon Select LMED, then choose the fingerprint reader.

C. WIRING DIAGRAM



D. WIEGAND OUTPUT DESCRIPTION

Chronograms



26-bit Wiegand Format Output

Place the ST1 jumper on 3

Structure and description of the code

Format 26-bit hexadecimal

The output format is 26-bit **Wiegand** (Signals: DATA1, DATA0 and CLOCK)
The frame is made of 26-bit and built as follow:

First parity: 1-bit – even parity for the first 12-bit

Code of the badge: 6 half byte represent the last 6 digit of the code (4 bit = 1 digit of the a code)
Each byte is transferred from bit 7 to bit 0.

Second parity: 1-bit – odd parity for the last 12-bit

Bit 1	Bit 2 … bit 25	bit 26
Even Parity on bit 2…bit13	Data (24 bit)	Odd Parity on bit 14… bit 25

Example: for code 0012051976

1	0000	0101	0001	1001	0111	0110	0
Parity 1	0	5	1	9	7	6	Parity 2

Example: the code transmitted 051976

Parity 1: 0 if the number of 1 in bit 2 to bit 13 is even
1 if the number of 1 in bit 2 to bit 13 is odd

Parity 2: 0 if the number of 1 in bit 14 to bit 25 is odd
1 if the number of 1 in bit 14 to bit 25 is even

30-bit Wiegand Format Output

Place the ST1 jumper on position 2

Structure and description of the code

The output format from the proximity reader is 30-bit wiegand (Signal: DATA1 and DATA0) and is structured as follow:
Signals output in open collectors with pull up in

30-bit hexadecimal format.

First parity : 1 bit – even parity for the first 14-bit

Code : A code is formed from 7 half byte.
Each byte is transferred from bit 7 to bit 0.

Second parity: 1 bit – odd parity for the last 14-bit

Bit 1	Bit 2 … bit 29	bit 30
Even Parity from bit 2…bit 15	Data (28-bit)	Odd Parity from bit 16… bit 29

Example: code 0012051976

1	0010	0000	0101	0001	1001	0111	0110	1
Parity 1	2	0	5	1	9	7	6	Parity 2

The code transmitted is 2051976

Parity 1: 0 if the number of 1 in bit 2 to bit 15 is even
1 if the number of 1 in bit 2 to bit 15 is odd

Parity 2: 0 if the number of 1 in bit 16 to bit 29 is odd
1 if the number of 1 in bit 16 to bit 29 is even

44- bit Wiegand Format Output

Place the ST1 jumper on position 1

Structure and description of the code

44-bit hexadecimal format

The output format from the proximity reader is 44-bit (Signal: DATA1, DATA0 and CLOCK) and is structured as follow:

Data: 10 digit code number hexadecimal MS Byte first
Each hexadecimal digit = 4 bit, MS Bit first
LRC: 4 bit = or restricted in between the digit of the data, MS Bit first

The frame is made of 44 bit and built as follow:

bit 1 …. Bit 40	Bit 41 … bit 44
Data MS Bit first	LRC

44 bit, hexadecimal format
Example : code 0012051976

LRC

0000	0000	0001	0010	0001	0101	0001	1001	0111	0101	0101

0	0	1	2	0	5	1	9	7	6	5

The code transmitted is 0012051976