

DIGigarde PLUS

Fingerprint Reader and Standalone Access Controller

User Guide

UM0063.GB Issue 1 10/04/2012

www.tdsi.co.uk

TDSi
Unit 10 Concept Park
Innovation Close
Poole
Dorset
BH12 4QT, UK

Tel: +44 (0) 1202 723535
Fax: +44 (0) 1202 724975

Sales Enquiries:	sales@tdsi.co.uk
General Enquiries:	info@tdsi.co.uk
Marketing Support:	marketing@tdsi.co.uk
Technical Support:	support@tdsi.co.uk

Foreword

Copy right © 2012 TDSi. All rights reserved.

Time and Data Systems International Ltd operate a policy of continuous improvement and reserves the right to change specifications, colours or prices of any of its products without prior notice.

Guarantee

For terms of guarantee, please contact your supplier.

Trademarks

Copyright © 2012 Time and Data Systems International Ltd (TDSi). This document or any software supplied with it may not be used for any purpose other than that for which it is supplied nor shall any part of it be reproduced without the prior written consent of TDSi.

Microsoft and Windows are registered trademarks of Microsoft Corporation.

All other brands and product names are trademarks or registered trademarks of their respective owners.

Cautions and Notes

The following symbols are used in this guide:



CAUTION! This indicates an important operating instruction that should be followed to avoid any potential damage to hardware or property, loss of data, or personal injury.



NOTE. This indicates important information to help you make the best use of this product.

Contents

1.	Introduction.....	1
1.1	About this manual.....	2
1.2	DIGIgarde PLUS layout.....	2
1.3	Basic concepts.....	3
1.3.1	User enrolment	3
1.3.2	User verification	3
1.3.3	Threshold	6
1.3.4	User ID numbers	6
1.3.5	Privilege levels.....	6
1.3.6	Log Definitions.....	7
1.4	How to use the fingerprint sensor	7
1.4.1	Correct positioning	7
1.4.2	Incorrect positioning	7
1.4.3	Common reasons for enrolment failure	8
1.5	LED indication.....	8
2.	Installation.....	9
2.1	Unpacking	9
2.2	Fitting the mounting plate	9
2.3	Connecting DIGIgarde PLUS	13
2.3.1	Preparing for connection.....	13
2.3.2	Wiring guide	14
2.3.3	Power connection	15
2.3.4	Wiegand/Magnetic Clock Data to a compatible ACU	15
2.3.5	Alarm connection.....	16
2.3.6	Lock and Sensor connection.....	16
2.4	Communication	18
2.4.1	TCP/IP.....	18
2.4.2	RS232.....	19
2.4.3	RS485.....	19
2.5	Power on	20
2.5.1	Display layout.....	20
2.5.2	Check In/Check Out.....	20
2.5.3	First tasks.....	20
3.	User Setup	21
3.1	Setting up Admin accounts	22
3.1.1	Privilege levels.....	22

3.1.2	Setting up an Admin account.....	22
3.2	Enrolment.....	24
3.2.1	Enrolling a fingerprint.....	25
3.2.2	Enrolling a password.....	27
3.2.3	Enrolling a fingerprint and password.....	28
3.3	Card enrolment.....	28
3.3.1	Enrol FP Card.....	29
3.3.2	Copy to Card.....	30
3.3.3	Register FP Card.....	30
3.3.4	Unregister FP Card.....	30
3.3.5	Delete FP Card.....	30
3.3.6	Copy Crd to Rdr.....	30
3.3.7	Move Rdr to Crd.....	30
4.	Device Settings.....	31
4.1	The Options menu.....	31
4.1.1	Date/Time.....	32
4.1.2	Language.....	32
4.1.3	Date Format.....	33
4.1.4	Daylight Saving Time.....	34
4.1.5	Wiegand format.....	35
4.1.6	Advanced Options.....	36
4.2	Power management.....	37
4.3	Communication options.....	37
4.4	Log options.....	38
4.5	LED mode.....	38
4.6	Data out type.....	38
5.	Standalone Mode.....	39
5.2	User Access Verification Flowchart.....	42
5.3	The Access Control menu.....	43
5.4	Defining time patterns.....	44
5.4.1	Assigning a Time Pattern to a Group.....	45
5.4.2	Assigning a Time Pattern to a User.....	45
5.5	User Access Options.....	45
5.5.1	Selecting the User.....	45
5.5.2	Assigning a user to a group.....	46
5.5.3	Setting a user's time patterns.....	46
5.5.4	Choosing a User's Verification Method.....	47
5.6	Access combinations.....	47

5.7	Lock and door sense	48
5.8	Alarm.....	49
5.8.1	Resetting the alarm.....	49
5.9	Defining Duress options.....	50
5.10	Anti Passback	51
5.10.1	Connection.....	51
5.10.2	Set up.....	52
5.10.3	Use.....	52
6.	System Information.....	53
6.1	Sys Info menu.....	53
6.2	Device Info menu	54
6.3	Free Space Info menu.....	54
7.	Maintenance.....	55
7.1	Cleaning the Keypad and Screen	55
7.2	Cleaning the Optical Sensor	55
8.	Troubleshooting	57
8.1	How to reset language back to English.....	57
8.2	How to reset the unit.....	57
8.3	How to clear admin privileges.....	57
8.4	When fingerprint verification fails.....	57
8.5	Communication failures	57
8.6	Display shows "Please try again" when no finger id presented for verification.....	58
9.	Appendices	59
9.1	Menu structure.....	59
9.2	Wiegand format.....	62
9.2.1	Wiegand format	62
9.2.2	26-bit Wiegand format.....	63

Figures

Figure 1	Removing the security screw from the base.....	9
Figure 2	Mark the fixing and cable hole positions.....	10
Figure 3	Drilling the holes: 6 mm for the fixings and 8 mm for the cable; fit the wall plugs.....	10
Figure 4	Securing the mount to the mounting surface.....	11
Figure 5	Feeding the cable and replacing the reader.....	12
Figure 6	Securing the DIGIgarde PLUS to the mounting plate.....	12
Figure 7	The DIGIgarde PLUS cable bundle.....	13
Figure 7	Alarm connection.....	16
Figure 7	Fail-Open or Fail-Locked door connections.....	17
Figure 8	Connecting a single DIGIgarde PLUS to a PC using RS-232.....	19
Figure 9	Example of a half-duplex (2-wire) RS-485 network.....	19
Figure 10	Access control options.....	40
Figure 11	Example of Access combination use.....	41

Tables

Table 1	Single factor verification modes.....	4
Table 2	Two factor verification modes.....	5
Table 3	Three factor verification modes.....	5
Table 4	Suggested Threshold Settings.....	6
Table 5	Cable Assignments.....	14
Table 6	Ethernet RJ-45 connector pin number (From left to right).....	18
Table 7	Possible fingerprint enrolment errors.....	26
Table 8	Card enrolment options.....	29
Table 9	Options menu categories.....	31
Table 10	Advanced options.....	36
Table 11	Communication options.....	37
Table 12	Log options.....	38
Table 13	Access Options menu.....	43
Table 14	User Access Options menu.....	46
Table 15	Lock and door sense settings.....	48
Table 16	Duress Options.....	50
Table 17	Sys Info options.....	53
Table 18	Device Info settings.....	54
Table 19	Free Space Info settings.....	54
Table 20	Wiegand pulse characteristics.....	62
Table 21	26-bit Wiegand field definition.....	63

1. Introduction

DIGIgarde PLUS is a combined fingerprint and card reader with integral backlit keypad providing PIN, Mifare card and fingerprint authentication modes in an attractive and cost-effective unit. With a high-resolution optical sensor and a fast matching algorithm it is suitable for the control of 'high traffic' access points. DIGIgarde PLUS units can also be used as Time & Attendance "clocking" stations.

- Operates stand-alone or in conjunction with Access Controller.
Use the reader to control the door or alternatively integrate it into a full access control system providing real-time event monitoring and central system programming & T&A - Use the T&A functionality of the reader to allow users to clock-in and clock out
- 1, 2 or 3 factor authentication
Gives you the flexibility to choose the level of security that matches your needs
- Built in Mifare™ Card reader
Allows storage of the fingerprint template on a smart card. Use the card for other applications
- Bypass card capability
Provides a means to grant access for those with badly damaged fingerprints
- High speed matching algorithm
Quickly scans and processes the fingerprint maximising user convenience
- Integrated with EXgarde
Manage the capture and distribution of templates from the same software used to monitor and program your access control system.
- Use the SDK to integrate DIGIgarde PLUS with other systems
- External reader input
Connect a third-party reader to allow a fingerprint template to be associated with a regular access control card
- Dual-colour LED
- Local programming interface
- IP 65 Rated
For internal or external mounting
- PoE powered
Removes the need to run a separate power cable to the reader
- APB
Allows two readers to be used to help prevent security breaches
- Custom message facility
Display user-specific messages on the reader to enhance user feedback
- High resolution optical sensor
Particularly suited for scanning small fingerprints
- TCP/IP, RS232 or RS485 connections
Supports a wide range of connection methods providing you with the connection choice for your installation
- 2 line white-on-black LCD display
Enhances user feedback and allows for simple programming
- Tamper protection
Be alerted immediately to the reader being removed from the wall.

1.1 About this manual

This manual describes the installation and configuration of DIGIgarde PLUS. It describes the verification options and the standalone capabilities of the device. The manual explains how to enrol users, set up groups and time patterns using the DIGIgarde PLUS keypad, its internal operating system and the DIGIgarde PLUS menu structure.

For information and instructions about the DIGIgarde PLUS software and how to program networked units, please refer to the DIGIgarde PLUS Software Guide.

For information about developing software for the DIGIgarde PLUS, please refer to the DIGIgarde PLUS SDK User Guide.

1.2 DIGIgarde PLUS layout



1.3 Basic concepts

This section describes the main concepts behind fingerprint identification using DIGIgarde PLUS:

- User Enrolment
- User Verification
- Match Threshold
- User ID Numbers
- Privilege Levels

1.3.1 User enrolment

You can enrol up to ten different fingerprints with each user ID.

When registering users, you should ideally enrol every finger and thumb. This avoids problems with users forgetting which finger has been enrolled or being unable to gain access because of any injury to the enrolled finger. At least two fingerprints should be enrolled, left and right index fingers, for example, to provide users with a 'backup'.

1.3.2 User verification

Verification is the process of assessing the identity of a user attempting to gain access through the DIGIgarde PLUS. This may involve checking some or all of the following: user ID, fingerprint, password (or PIN) or smart card.

1:1 and 1:N fingerprint verification

There are two basic types of fingerprint verification:

- If the user is required to enter their ID, then the DIGIgarde PLUS is only required to match the scanned fingerprint against the template registered under the User's ID. This is called 1:1 verification.
- If a user is not required to input their ID, the DIGIgarde PLUS must then match the scanned fingerprint against all the templates in its database. This is termed 1:N verification.

The verification process may also involve checks of an input password. DIGIgarde PLUS shows whether the user has been identified successfully and stores the result in its internal memory.

Verification factors

The DIGIgarde PLUS Fingerprint reader supports single, dual and three factor verification modes. Table 1, Table 2 and Table 3 provide a description of the verification modes and shows how to use them. In the following table and in the DIGIgarde PLUS menu, the following symbols are used:

/ means OR; + means AND

FP: Fingerprint; **PW**: Password (5-digit); **ID**: User ID (9-digit); **RF**: smart card

Table 1 **Single factor verification modes**

Mode	Description
FP	Only verify fingerprint using one of the following methods: <ul style="list-style-type: none"> Enter ID; verify FP (1:1 verification) Verify FP (1:N verification) Present RF card; verify FP (1:1 verification)
ID	Only verify the User ID <ul style="list-style-type: none"> Enter ID through keypad
PW	Only verify the password <ul style="list-style-type: none"> Enter ID; enter PW Present RF card and enter PW
RF	Only verify the RF card <ul style="list-style-type: none"> Present RF card
FP/PW	Verify fingerprint OR password <ul style="list-style-type: none"> ID and FP (1:1) FP (1:N) Enter ID; enter PW Present RF card; enter PW
FP/RF	Verify fingerprint or RF card <ul style="list-style-type: none"> Enter ID; verify FP (1:1 verification) Verify FP (1:N verification) Present RF card
PW/RF	Verify password or RF card <ul style="list-style-type: none"> Present RF card Enter ID; enter PW
FP/PW/RF	Verify fingerprint or password or RF card <ul style="list-style-type: none"> Enter ID; verify FP (1:1 verification) Verify FP (1:N verification) Enter ID; enter PW Present RF card

Table 2 Two factor verification modes

Mode	Description
FP&ID	Verify fingerprint and ID <ul style="list-style-type: none"> Enter ID; verify FP (1:1 verification) Present RF card; verify FP (1:1 verification)
FP&PW	Verify the fingerprint and password <ul style="list-style-type: none"> Verify fingerprint (1:N verification) and enter PW Enter ID; verify fingerprint (1:1 verification); enter PW Present RF card; enter PW; verify FP (1:1 verification)
FP&RF	Verify the fingerprint and RF card <ul style="list-style-type: none"> Present RF card and verify FP (1:1 verification) Verify FP (1:N verification and present RF card) Enter ID; verify FP (1:1 verification); present RF card
FP& ID / RF	Verify the fingerprint and ID or Fingerprint and RF <ul style="list-style-type: none"> Verify FP (1:N verification); enter ID Verify FP (1:N verification); present RF card Enter ID; verify FP (1:1 verification); enter ID Enter ID; verify FP (1:1 verification); present RF card

Table 3 Three factor verification modes

Mode	Description
FP&PW&RF	Verify the fingerprint, password and RF card <ul style="list-style-type: none"> Verify FP (1:N verification); enter PW; present RF card Enter ID; verify FP (1:1 verification); enter PW; present RF card Present RF card; enter PW; verify FP (1:1 verification)
FP&ID&PW	Verify the fingerprint, ID and Password <ul style="list-style-type: none"> Enter ID; enter PW; verify FP (1:1 verification) Present RF card; enter ID; enter PW; verify FP (1:1 verification)

1.3.3 Threshold

The quality of scanned fingerprints can be variable. This opens up the possibility of two types of verification failure:

- Valid users are rejected. This is called **False Rejection**. The False Rejection Rate (FRR) is the probability that DIGIgarde PLUS will fail to identify an enrolled user, or verify their legitimate identity.
- An imposter is mistakenly accepted because of the similarity of their fingerprint to that of a registered user. This is termed **False Acceptance**. The False Acceptance Rate (FAR) is the probability that DIGIgarde PLUS will incorrectly verify an individual or will fail to reject an impostor.

To minimize these effects, DIGIgarde PLUS uses a **Threshold** value to establish a balance between False Acceptance and False Rejection. A high threshold value reduces the chances of false acceptance but increase the probability of false rejection. The default Threshold value is 35 for 1:N matching and 15 for 1:1 matching. Clearly, the chance of a false acceptance is much less when a user ID is required since the DIGIgarde PLUS is only comparing the scanned fingerprint with one template.

The threshold can be set for all users. Raising the threshold increases security, while lowering it increases pass rate.

For a user whose fingerprint verification is difficult, you can either reduce the threshold or adopt ID & Fingerprint verification (1:1 verification) – see page 45.

Table 4 Suggested Threshold Settings

FRR	FAR	1:N	1:1
High	Low	45	25
Middle	Middle	35	15
Low	High	25	10

1.3.4 User ID numbers

During enrolment, DIGIgarde PLUS assigns a User ID Number to each user. This ID can be used to call up the fingerprint template (1:1 verification) and/or password each time that verification is requested.

A user can enter their ID number using the keypad or it can be called up from an RF Card or Mifare Card.

1.3.5 Privilege levels

DIGIgarde PLUS recognizes four Privilege levels:

- **Users**
People whose identity must be verified to gain access to a facility or to have their attendance recorded.
- **Enrollers**
DIGIgarde PLUS users who are authorized to enrol or delete users in the system.
- **Managers**
Additional powers except set advanced options and enrol manager or above privilege users.

Supervisors

Users with access to all DIGIgarde PLUS functions including system settings.



NOTE. During the initial setup, an Enroller may create Manager and Supervisor accounts. Similarly, a Manager may create a Supervisor account. However, once these accounts exist, only a Supervisor may create or edit Manager and Supervisor accounts.

1.3.6 Log Definitions

The DIGIgarde PLUS records the following data:

Attendance Log Shows all attendance transactions.

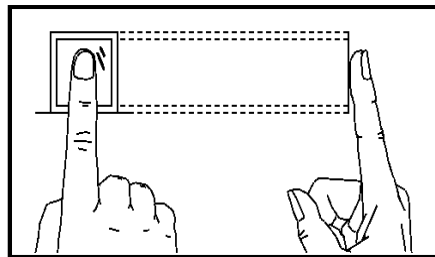
Super Log Documents system changes.

1.4 How to use the fingerprint sensor

The quality of the fingerprint verification process depends on the ability of the user to correctly position their finger on the scanning window. The finger should be placed centrally and flat and not be moved during the 2-3 seconds of the scan.

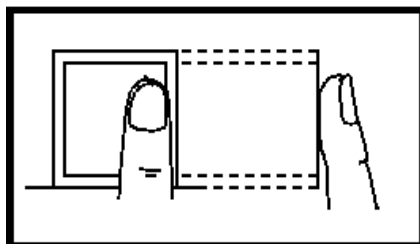
1.4.1 Correct positioning

Finger aligned, centrally positioned and flat on the scanning window.

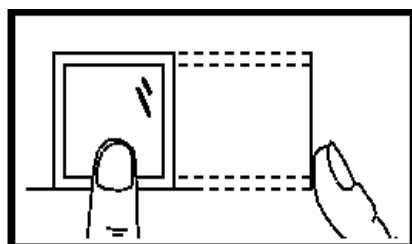


1.4.2 Incorrect positioning

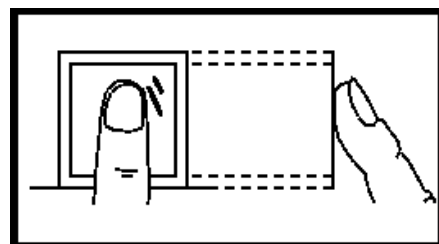
Too far to one side/not central



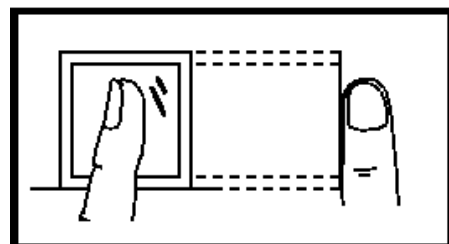
Finger not fully on window



Raised finger/not flat on scanning window



Finger side on or at an angle



1.4.3 Common reasons for enrolment failure

This section lists some of the common reasons for enrolment failure

Problem	Remedy
Finger is too dry or dirty	Rub the finger in the palm of your hand to moisten/clean it.
Finger applied too lightly	Place a finger firmly and flat on the sensor surface.
Finger positioned incorrectly	Your finger should cover most of the sensor window.
Finger removed or moved during scan	Hold your finger still and do not slide it on the sensor window until the verification process is complete
Injury or wear has changed the fingerprint pattern	If the problem occurs with 1:N verification, try 1:1 verification, if this is an available. Contact the administrator. You may need to enrol another finger or use a password verification method instead.

Enroller's guidelines

When enrolling, we recommend you enrol users with their left or right index or middle finger. Check the fingers for any injuries or wear.

If the user's fingers are small, it may be preferable to use a thumbprint.

Few people's fingerprint quality is too poor to verify but in difficult cases it is advisable to use an ID & fingerprint verification method with the threshold reduced accordingly. In extreme cases, use password verification to avoid fingerprint verification problems.

1.5 LED indication

The DIGIgarde PLUS unit has a red/green status LED in its top-left corner. This provides information about the verification process.

Normal	Red light flashes
Verification failure	Red light on constant for 3 second
Verification successful	Green light constant for duration of 'Lock Open' state.

2. Installation

2.1 Unpacking

Carefully unpack the DIGIgarde PLUS. The box contains the following:

- DIGIgarde PLUS unit
- CD with operating software, this manual, SDK software.
- Mounting template
- Quick start guide
- Cable assembly
- Ferrite ring
- Tool for security screw

To install and operate the DIGIgarde Plus software, please refer to the DIGIgarde PLUS Software Guide.

- Fixing plugs and screws
- Suppression diode

2.2 Fitting the mounting plate

Fixing plugs and screws are supplied for mounting into brick or concrete. For mounting onto other materials, please obtain suitable fixings for that material.

1. Using the tool supplied, remove the security screw from the bottom of the reader. Remove the mount (rear cover) from the reader.

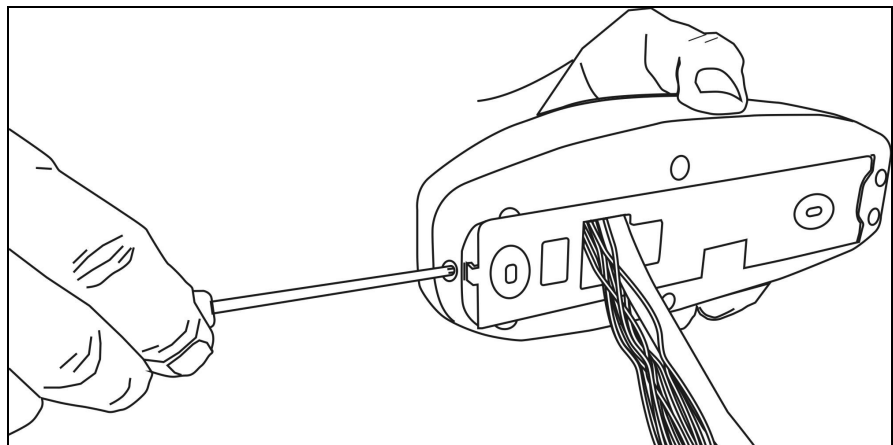


Figure 1 Removing the security screw from the base

2. Position the mounting plate against the wall or door frame and, using a pencil, mark the positions of the three holes.

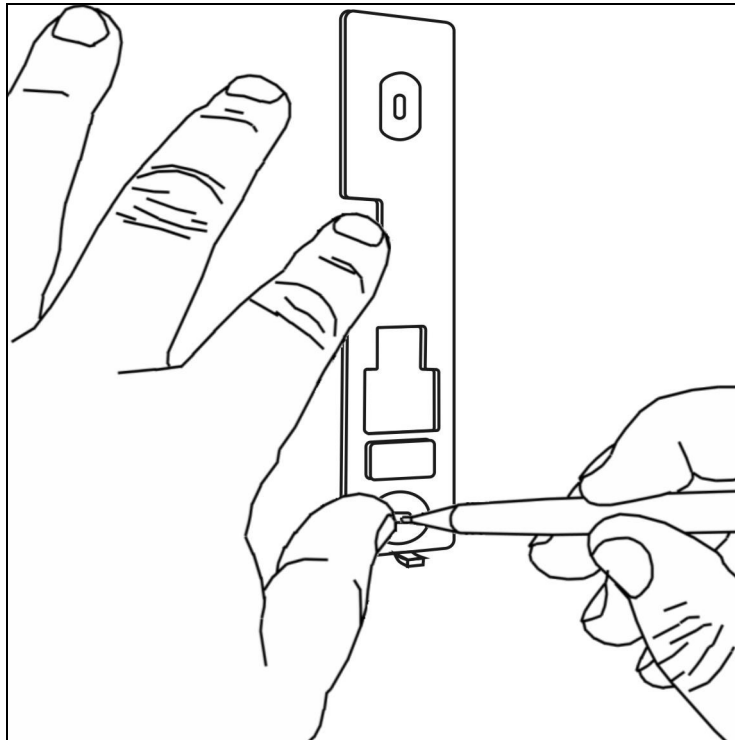


Figure 2 Mark the fixing and cable hole positions



CAUTION! Check for internal pipes and wires.

3. Drill two 6 mm holes for the wall fixings and a single 10 mm hole for the cable. Fit the wall plugs into the 6 mm holes.

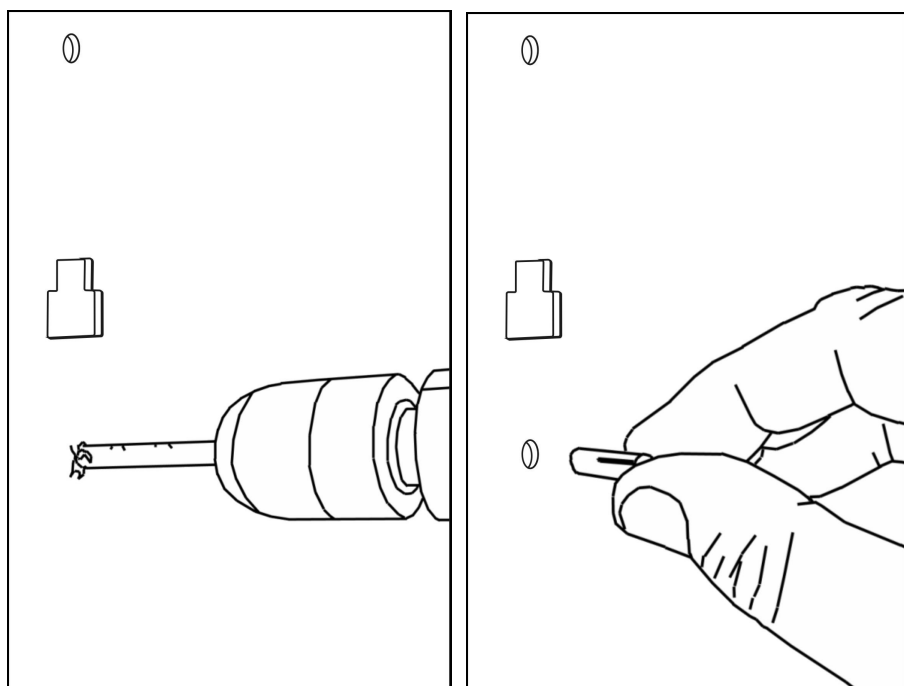


Figure 3 Drilling the holes: 6 mm for the fixings and 8 mm for the cable; fit the wall plugs

4. Place the mounting plate on the wall and secure it in position with the screws. Use a spirit level to ensure that the mounting plate is true.

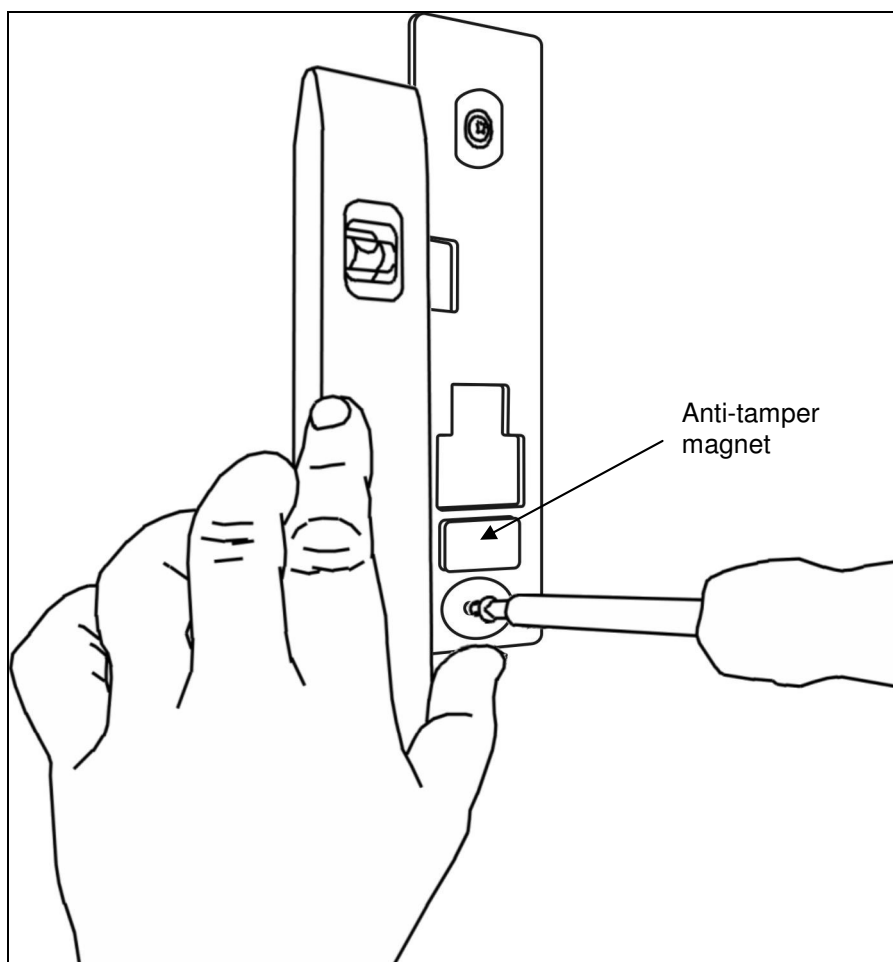


Figure 4 Securing the mount to the mounting surface

5. Ensure that the anti-tamper magnet is in position below the cable access hole.

6. Feed the cable into the wall and hook the top of the DIGIgarde PLUS onto the mount.

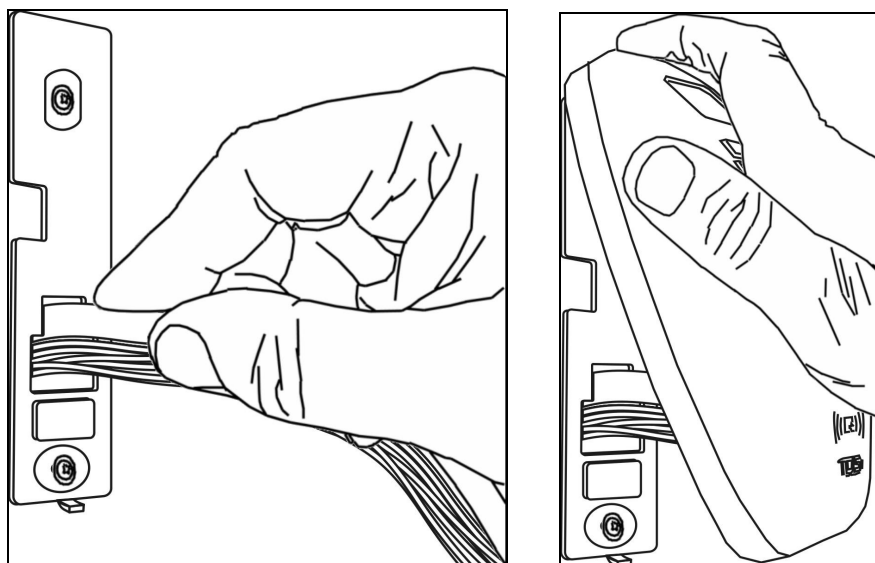


Figure 5 Feeding the cable and replacing the reader

7. Lower the DIGIgarde PLUS into place and fit the security screw into the bottom of the unit. Tighten the screw only sufficiently to retain the main housing against the back plate.



CAUTION! Do not over-tighten the screw.

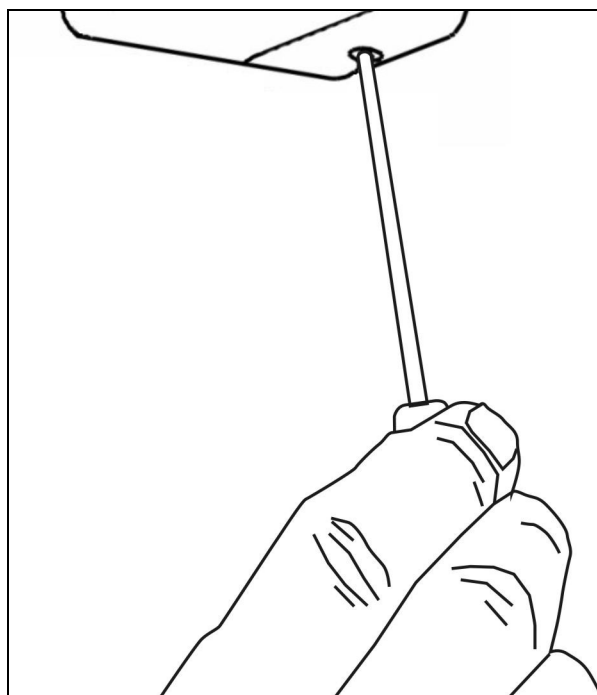


Figure 6 Securing the DIGIgarde PLUS to the mounting plate

8. Fit the supplied ferrite ring around the wire bundle for EMC protection (see Figure 7).

2.3 Connecting DIGIgarde PLUS

This section describes the connection of DIGIgarde PLUS to access control units, other DIGIgarde PLUS units, door locks and sensors, alarms and a PC.

2.3.1 Preparing for connection

The items required for setup:

- ✓ DIGIgarde PLUS complete with connection cable.
- ✓ Magnetic ring for EMC protection (see below).
- ✓ A suitable power supply with an output voltage of 10 to 14 VDC capable of supplying 500 mA (peak). Note that the power supply from the access control unit can be used if it is capable of providing a peak of 500 mA.
- ✓ Optional - A TDSi access control unit or other suitable controller featuring a Wiegand input port.



CAUTION! Please read this section carefully as incorrect wiring could cause irreparable damage to DIGIgarde PLUS and invalidate the warranty. Check all wiring before connecting power to the unit. Ensure the correct supply voltage is set before powering DIGIgarde PLUS and connected devices.

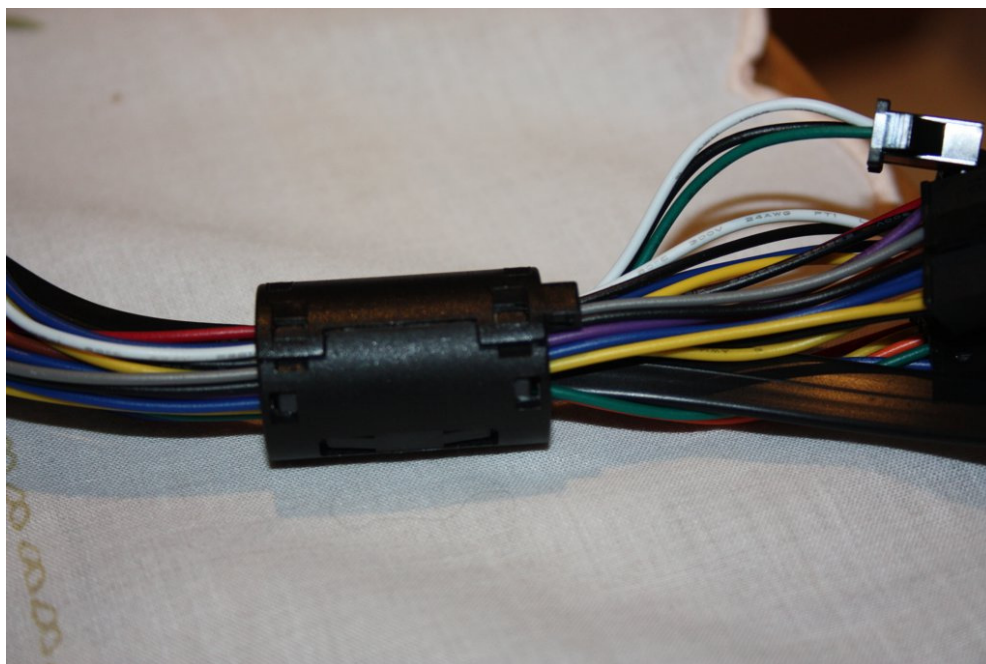





























Figure 7 The DIGIgarde PLUS cable bundle with ferrite ring

2.3.2 Wiring guide

DIGIgarde PLUS can be connected to other devices (access control units, lock, door sensor, alarm, host PC etc) through the colour-coded and labelled connection cables. In addition to the connections described in Table 5, there is also a pre-configured RJ-45 connector.

Table 5 Cable Assignments

Label	Wire Colour		Signal	Description
Power	Black		0V	Power GND
	Red		+12V	Power Input
WG IN	Black		GND	GND
	White		WD0-IN	Wiegand Input, Data 0
	Green		WD1-IN	Wiegand Input, Data 1
WG OUT	Yellow		WD0-OUT	Wiegand Output, Data 0
	White		WD1-OUT	Wiegand Output, Data 1
	Black		GND	Wiegand GND
	Blue		LED	LED
Lock	White		SENSOR	Door Sensor power
	Black		GND	Door Sensor ground
	Grey		BUTTON	Egress button
	Blue		NO1	Normally Open
	Red		COM1	Common
	Yellow		NC1	Normally Closed
Alarm	Orange		ALARM NO2	Alarm (Normally Open)
	Green		ALARM COM2	Alarm (Common)
RS485-2	Blue		RS-485A-2	RX+, RS-485-2 level
	Yellow		RS-485B-2	RX-, RS-485-2 level
RS232	Black		RS-232 0V	RS-232 0V
	Grey		RS-232 RX	Receive Data, RS-232C level
	Purple		RS-232 TX	Transmit Data, RS-232C level
RS485-1	Blue		RS-485A-1	RX+, RS-485-1 level
	Yellow		RS-485B-1	RX-, RS-485-1 level
	Black		GND	RS-485 GND
RS485RES	Brown		RS-485RES	Link wires to provide termination resistor (see page 19).
	Brown		RS-485RES	

2.3.3 Power connection

You can power the unit directly using a DC supply or by using PoE (Power over Ethernet).

Using a DC power supply

To power the unit, connect red and black wires labeled **Power** to a power supply rated at 10 to 14 VDC and capable of supplying a current of 500mA.

Label	Wire Colour	Signal	Description
Power	Black	0V	Power GND
	Red	+12V	Power Input

Using PoE

Connect the DIGIgarde PLUS to a PoE-enabled network device such as an Ethernet switch using the RJ45 connector and an appropriate CAT5 (or higher) cable.. You can also 'inject' power into the network cable using a midspan power supply or PoE injector.

2.3.4 Wiegand/Magnetic Clock Data to a compatible ACU

Connect the wire **WD0-OUT** on the reader to **Data 0** on the access control unit and the wire **WD1-OUT** on the reader to **Data 1** on the access control unit.

Label	Wire Colour	Signal	Description
WG OUT	Yellow	WD0-OUT	Wiegand Output, Data 0
	White	WD1-OUT	Wiegand Output, Data 1
	Black	GND	Wiegand GND
	Blue	LED	LED

2.3.5 Alarm connection

To use an external alarm (see page 16) for indicating repeated failed verification, an unexpected door open/closed state, duress access or for help indication, connect the alarm power lines to the marked orange and green wires.

Label	Wire Colour	Signal	Description
Alarm	Orange	ALARM -	Alarm -
	Green	ALARM +	Alarm +

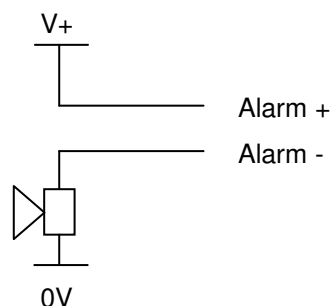


Figure 8 Alarm connection

2.3.6 Lock and Sensor connection

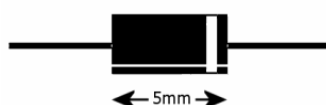
CAUTION! A suppressor MUST be fitted at each lock (see below). Suitable suppressors (1N4003 diodes) are provided with each MICROgarde controller and can be purchased separately from TDSi.

For each lock, allow 50% more than stated power rating. For example, if the lock has a rating of 500mA, use a 750mA minimum supply. If the lock has a higher current rating than the lock relay (2A?), use a secondary relay.

Never run the power supply and sensor or communication lines in the same cable.

Label	Wire Colour	Signal	Description
Lock	White	SENSOR	Door Sensor power
	Black	GND	Door Sensor ground
	Grey	BUTTON	Egress button
	Blue	NO	Normally Open
	Red	COM	Common
	Yellow	NC	Normally Closed

Fitting a suppressor



Fit a suppressor across the lock supply as close to the lock as possible with the white band end connected to the positive side of the supply.

Fail-Open or Fail-Locked Connection

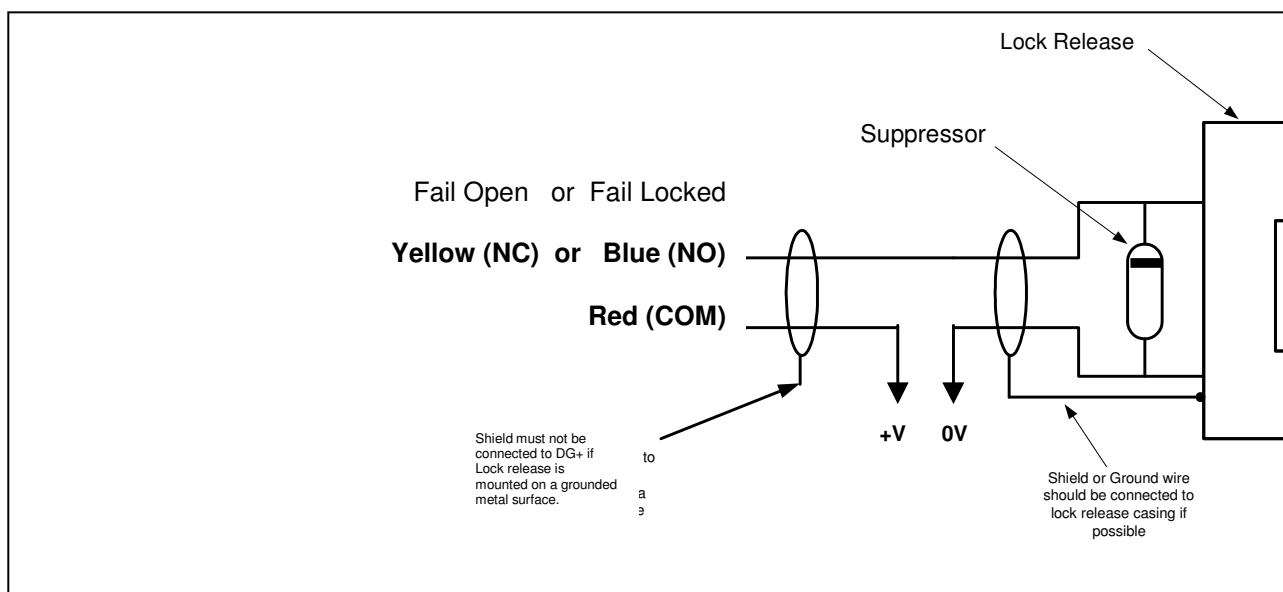


Figure 9 Fail-Open or Fail-Locked door connections

In a Fail-Open (or Fail-Safe) connection, the door is opened in the event of a power failure. In a Fail-Locked connection, the door is locked in the event of a power failure.

Door Sensor Connection

Connect the door sensor to the White (**SENSOR**) and Black (**GND**) wires in the Lock bundle.

Most door sensors have contacts that are closed circuit when the door is closed. Please contact TDSi if you have sensors that are open circuit when the door is closed.

Egress button

Connect the Egress button to the Grey wire (**BUTTON**) and the red **COMMON** wire in the LOCK bundle. This will activate the lock relay and open its associated door.

2.4 Communication

DIGIgarde PLUS can be connected to a TCP/IP or RS485 network or directly to a PC using RS-232.

2.4.1 TCP/IP

DIGIgarde PLUS is supplied with a connected and configured PoE-capable RJ45 socket (for PIN assignments, see Table 6).

Power over Ethernet (PoE) extends the functionality of Ethernet by supplying reliable DC power over the same Category 5/5e twisted-pair cable that currently carries Ethernet data. PoE can supply reliable power to low power Ethernet network devices such as wireless access points (WAP) and security cameras.

To use PoE to power the DIGIgarde PLUS, you must connect the unit to a PoE-enabled network device such as an Ethernet switch. Alternatively, power can be injected into the cable from a midspan power supply or PoE injector.

Table 1 shows the Ethernet RJ45 connector pin assignments for the DIGIgarde PLUS. Pins 4&5 provide the DC supply with pins 7&8 being the GND connections. Data is communicated on pins 1&2 and pins 3&6.

Table 6 Ethernet RJ-45 connector pin number (From left to right)

Number	Wire Colour	Purpose
1	White/Orange	TX+
2	Orange	TX-
3	White/Green	RX+
4	Blue	Power
5	White/Blue	Power
6	Green	RX-
7	White/Brown	GND
8	Brown	GND

2.4.2 RS232

Connect **RS-232 RX**, **RS-232 TX** and **RS-232 0V** on the reader to **TX**, **RX** and **0V** of the PC serial port respectively. Please refer to Figure 10.

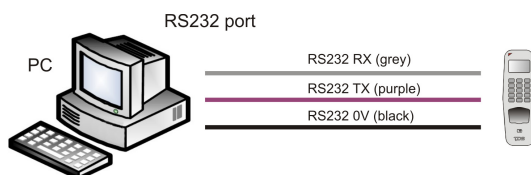


Figure 10 Connecting a single DIGIgarde PLUS to a PC using RS-232

2.4.3 RS485

Half duplex (2-wire)

For a half-duplex (2-wire) network operation a single pair of twisted wires in a shielded cable is required. For every device in the half-duplex network, connect **TX+** to **RX+** and **TX-** to **RX-** locally before connecting to the network. At the end of the network, termination resistors of 120Ω should be connected between the **+ve** and **-ve** terminals.



NOTE. Each unit must have a different Device number (set in **Menu > Options > Comm Opt > Dev Num**, see page 37).

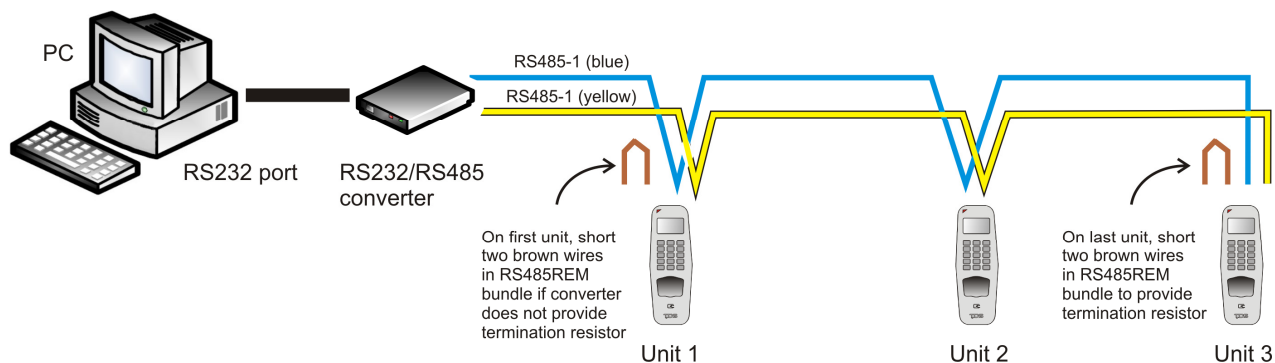
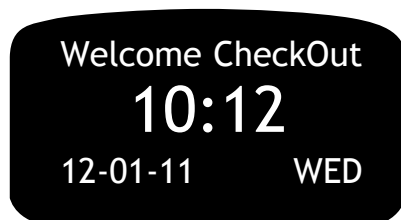


Figure 11 Example of a half-duplex (2-wire) RS-485 network

2.5 Power on

2.5.1 Display layout

When you first apply power to the unit it will display the TDSi logo. After a few seconds, DIGIgarde PLUS displays the Welcome screen:



2.5.2 Check In/Check Out

The Welcome screen shows the time and date and the CheckIn/CheckOut status of the unit.

- To change the unit to a **CheckIn** status, press the ▲ key.
- To change the unit to a **CheckOut** status, press the ▼ key.

2.5.3 First tasks

Setting the date and time	page 32
Changing the language	page 32
Creating an administrator's account	page 22
Enrolling a user	page Error! Bookmark not defined.
Setting up time patterns	page 44
Assigning a user to a group	page 46

3. User Setup

This chapter describes how to enrol and verify users.

The following topics are included:

- Setting up the Enroller account and, optionally, Manager and Administrator accounts.
- Enrolling a user
- Testing an enrolment
- Enrolling an auxiliary fingerprint for user
- Verifying your identity
- Prompts for successful enrolments

3.1 Setting up Admin accounts

The first time the DIGIgarde PLUS is powered up, there are no user accounts. Your first step should be to create password-protected enroller and administrator accounts.

3.1.1 Privilege levels

DIGIgarde PLUS recognizes four Privilege levels:

- **User**
 People whose identity must be verified to gain access to a facility or to have their attendance recorded.
- **Enroller**
 DIGIgarde PLUS users who are authorized to enrol or delete users in the system.
- **Manager**
 Additional powers except set advanced option and enrol manager or above privilege users.
- **Admin**
 Supervisory role with access to all DIGIgarde PLUS functions including system settings.



NOTE. During the initial setup, an Enroller may create Manager and Admin accounts. Similarly, a Manager may create a Admin account. However, once these accounts exist, only an Admin may create or edit Manager and Admin accounts.

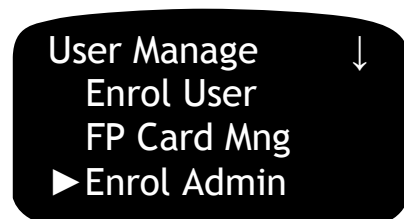
3.1.2 Setting up an Admin account

To set up an Admin, Manager or Enroller account:

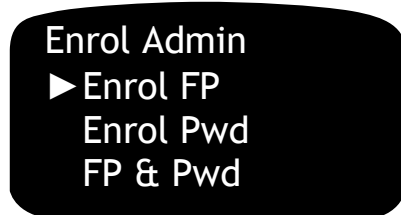
1. Press the **Menu** button.



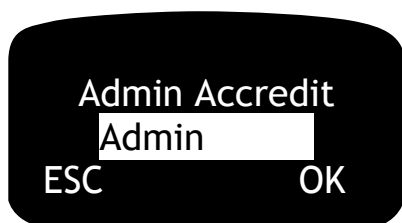
2. Press the **OK** button to select the *User Manage* menu option.



3. In the *User Manage* menu, use the ▲▼ keys to select the *Enrol Admin* option. Press the **OK** button to select the *Enrol User* menu option.



4. In the *Enrol Admin* menu, use the ▲▼ keys to select the enrolment method:
Enrol FP enrol a fingerprint to a new or existing user.
Enrol PWD Enrol a password to a new or existing user.
FP & Pwd Enrol a fingerprint and password to a new or existing user.
5. Press the **OK** button. The *Admin Accredit* screen is displayed. Use the ▲▼ keys to choose the management role for the user to be enrolled.



6. Press the **OK** button. Now follow the procedures described in the following sections:
- Enrolling a fingerprint
 - Enrolling a password



CAUTION! If the admin is unable to log in, it will be necessary to carry out a factory reset of the unit to be able to carry out any admin functions (see page 57).



NOTE. If you change the verification mode of group 1, the default user group, make sure you do not lock yourself out of the menu. For example, if you set group 1 to PW verification, enrol yourself as Admin with PW-only verification, and subsequently change group 1 to FP verification, you will be unable to get back in to the menu.

3.2 Enrolment

The DIGIgarde PLUS provides four ways to enrol a user:

- Fingerprint Enrolment.
- Password Enrolment.
Note. On the DIGIgarde PLUS, a 'Password' is a 5-digit number.
- Combined Fingerprint and Password Enrolment.
- Mifare card (see page 28).

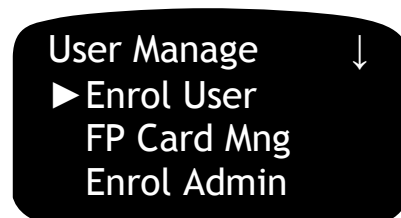
You can choose the enrolment method to suit a particular user. For example, a user with poor quality fingerprints can be given a password verification option.

To enrol a user:

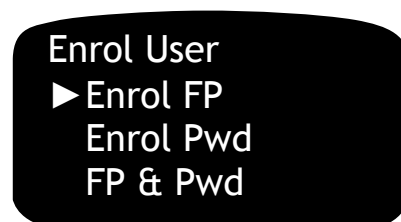
1. Press the **Menu** button.
If you have registered an Administrator, Manager or Enroller account, you are prompted to verify your identity (see page 7). After you have done this, press the **Menu** button again.



2. Press the **OK** button to select the *User Manage* menu option.



3. Press the **OK** button to select the *Enrol User* menu option.



4. Use the ▲ ▼ keys to select the required option:

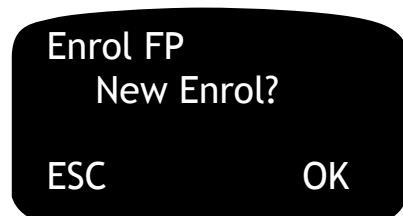
Enrol FP	enrol a fingerprint to a new or existing user.
Enrol PWD	Enrol a password to a new or existing user.
FP & Pwd	Enrol a fingerprint and password to a new or existing user.

3.2.1 Enrolling a fingerprint

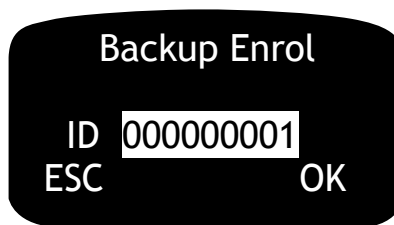
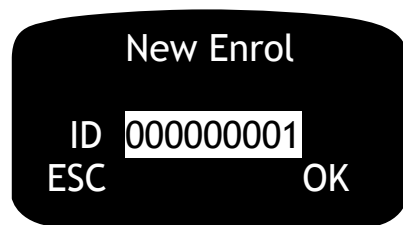
You can enrol up to ten different fingerprints with each user ID.

When registering users, you should ideally enrol every finger and thumb. This avoids problems with users forgetting which finger has been enrolled or being unable to gain access because of injury to the enrolled finger. This can be time-consuming but at least two fingerprints should be enrolled, left and right index fingers, for example, to provide users with a 'backup'.

1. Select the **Enrol FP** option and press the **OK** button.



2. If the fingerprint is for a new user account, press the **OK** button. To add an additional fingerprint to an existing user account, press the **ESC** button. The procedure is the same, in both cases.



3. DIGIgarde PLUS displays the ID it will assign as the User ID for this account. The ID is a 9-digit number. As you enrol users, DIGIgarde PLUS automatically increments the ID starting from 000000001 for the first new user. If you want to enter a specific number (avoiding existing User IDs), type it in using the keypad starting with the highest digit.
4. Click on the **OK** button to continue. The user ID is now appended with a number to indicate the order of fingerprints enrolled by this user. 0 (zero) corresponds to the first fingerprint, 1 the second, and so on, up to 9.
5. Ask the user to place their finger on the scanning window.



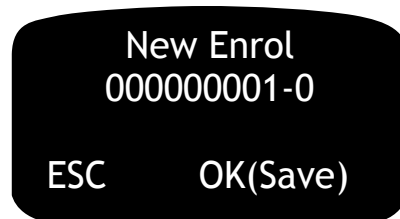
6. The scanning process takes a few seconds. When this is complete, the DIGIgarde PLUS beeps and prompts the user to remove their finger. Repeat this procedure for two further scans.



7. If the enrolment is successful, DIGIgarde PLUS prompts you to save the scanned fingerprint. Press the **OK** button to save the fingerprint template and create the user account or press **ESC** to discard the scans and cancel the enrolment.



NOTE. If you forget to press the **OK** button the template will not be saved.



If you want to enrol another user, press the **OK** button.

If you want to enrol a backup fingerprint for the same user, press **ESC**.

If you want to return to the main menu, press **ESC** twice.

Table 7 Possible fingerprint enrolment errors

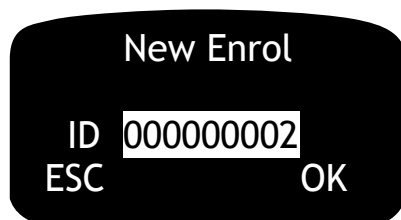
Screen message	Voice prompt	Description
Input again	"Please try again"	Error during scanning. For example, a different finger was used for one of the scans.
FP Enrolled Alrd	"Duplicate finger"	The fingerprint has already been enrolled to an existing user ID.

3.2.2 Enrolling a password

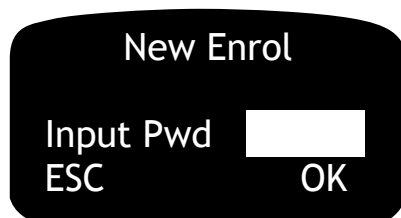
To enrol a password, follow the first steps described in the previous section. On the *Enrol User* menu, use the ▲▼ keys to select the *Enrol Pwd* option. Click on the **OK** button.



1. If the password is for a new user account, press the **OK** button (to add a fingerprint to an existing user account, press the **ESC** button).
2. DIGIgarde PLUS displays the ID it will assign as the User ID for this account. The ID is a 9-digit number. As you enrol users, DIGIgarde PLUS automatically increments the ID starting from 000000001 for the first new user. If you want to enter a specific number, type it in using the keypad starting with the highest digit.



3. Click on the **OK** button to continue.

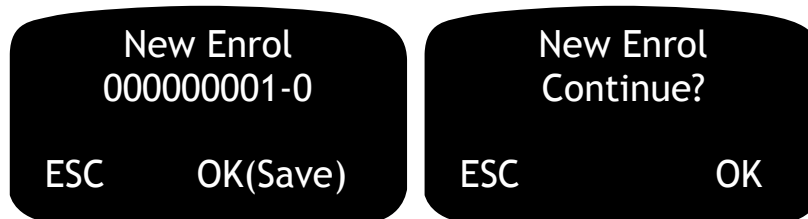


4. The password is a 5-digit number.



5. Confirm the password by entering it a second time. If you make a mistake the screen will be redisplayed.

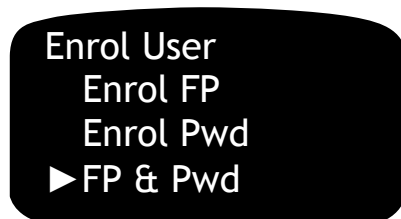
6. DIGIgarde PLUS prompts you to save the password and confirm the enrolment. Press the **OK** button or press **ESC** to cancel the enrolment.



7. If you want to enrol other new users, press the **OK** button when prompted to continue. Otherwise, press **ESC** to return to the *Enrol User* menu.

3.2.3 Enrolling a fingerprint and password

To enrol a fingerprint and password for the same user, follow the first steps described in the previous section. On the *Enrol User* menu, use the ▲ ▼ keys to select the *FP & Pwd* option. Click on the **OK** button.

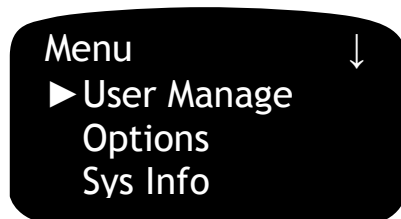


Now follow the steps on pages x and x respectively.

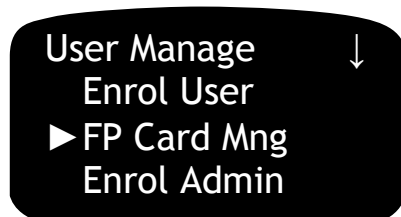
3.3 Card enrolment

To enrol a user and set up smart card authentication:

1. Press the **Menu** button.
If you have registered an Administrator, Manager or Enroller account, you are prompted to verify your identity. After you have done this, press the **Menu** button again.



2. Press the **OK** button to select the *User Manage* menu option.



- Press the **OK** button to select the *FPCard Manage* menu option.

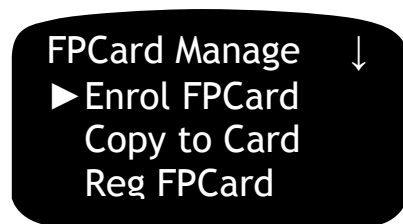


Table 8 Card enrolment options

Command	Before command		After command	
	DIGIgarde PLUS	Card	DIGIgarde PLUS	Card
Enrol FP Card			ID	Template,ID
Copy to Card	Template,ID		Template,ID	Template,ID
Register FP Card		Template,ID	ID	Template,ID
Unregister FP Card	Template,ID	Template,ID	ID	Template,ID
Delete FP Card	No action	Template,ID	No action	
Copy Crd to Rdr	ID	Template,ID	Template,ID	Template,ID
Move Rdr to Crd	Template,ID		ID	Template,ID

3.3.1 Enrol FP Card

Register a user by enrolling their fingerprint and storing the template in a Mifare card. The template is not stored locally on the DIGIgarde PLUS and the unit will be unable to authenticate the user without their card.

To enrol a user with a smart card:

- Select **Enrol FPCard**.
- Enter a new user ID or Press **OK** to accept the spare ID offered by the DIGIgarde PLUS. Press **OK**.
- Enter Special **N** to continue or **Y** to make this a by-pass card.
- Enrol the user's fingerprint as described on page 25.
- If this is successful, the "*Continue?*" prompt is displayed. Press **OK** to enrol further fingerprints in the same manner or press **ESC** to continue.
- When prompted to do so ("*Show the card*"), present the Mifare card to the front of the DIGIgarde PLUS. The fingerprint information is written to the card and a "Succ" message is displayed.



NOTE. Ensure that you keep the card on the reader until the template has been written and the "Success" message has been displayed.

3.3.2 Copy to Card

Copy the fingerprint template and user information from an existing account to the Mifare card. The template remains within the DIGIgarde PLUS and a user will be able to log in without their card.

3.3.3 Register FP Card

Create a user account from the information stored on a Mifare card. The fingerprint template remains on the card and is not stored in the DIGIgarde PLUS. This option provides a quick way to add a user to multiple readers.

3.3.4 Unregister FP Card

Delete the user account registered on the DIGIgarde PLUS based upon the information stored on the Mifare card.

3.3.5 Delete FP Card

Erase the Mifare card.

3.3.6 Copy Crd to Rdr

Copy a fingerprint template from the Mifare card to the DIGIgarde PLUS.

3.3.7 Move Rdr to Crd

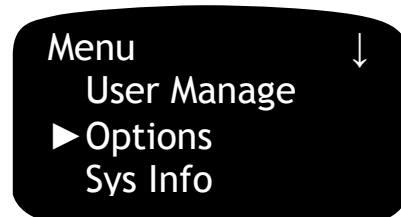
Move the fingerprint template from the reader to the Mifare card (erasing the information on the reader).

4. Device Settings

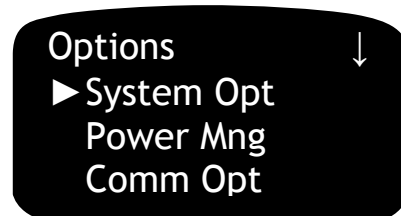
4.1 The Options menu

To alter any of the DIGIgarde PLUS settings, press the **Menu** button and, if necessary, verify your identity.

1. Press the ▼ key to select *Options*.



2. Press the **OK** button. The *Options* menu is displayed.



3. The system options are divided into the following categories:

Table 9 Options menu categories

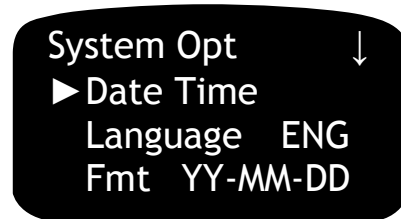
Options menu category	Use
System Opt	Date and time settings, on-screen language, date format, lock timings.
Power Mng	Set the time for the unit to enter its hibernation mode after a period of inactivity.
Comm Opt	Configure communications settings, for example, baud rate, IP address
Log Opt	Set alarm notifications for data logs approaching full capacity.
LED Mode	Set unit in Standalone or Controller (ACU controlled) mode.
Data Out Type	Choose protocol for data output: Wiegand or Magnetic.
Access Options	Set time periods and define user groups.
Auto Test	Run internal tests for screen defects, voice prompts, fingerprint reader, keypad operation and real-time clock.

To view further *Options* menu categories, use the ▼ key to scroll down past the first three categories.

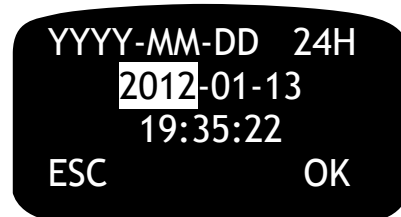
4.1.1 Date/Time

To change the Date/Time setting:

1. From the *Options* menu, select *System Opt*. Press the **OK** button.



2. With *Date Time* selected, press the **OK** button.



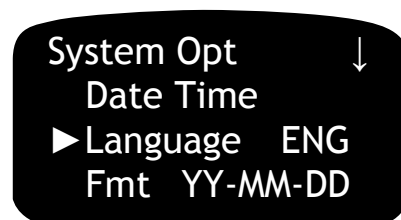
3. The date format is shown across on the top line of the screen. This cannot be changed here. To change the date format, return to the *System Opt* menu and select the *Fmt* option (see below).
4. The date is shown on the second line with the time on the third line.
5. To navigate between the various fields: year, month, day, hours, minutes, seconds use the **▲▼** keys.
6. When selected in this way, edit a value by typing the new value on the keypad.

Repeat this procedure for the other fields and then press the **OK** button to confirm your changes.

4.1.2 Language

To change the unit's language:

1. From the *Options* menu, use the **▲▼** keys to select *Language*. Note that the code of the currently selected language is displayed alongside. Press the **OK** button.



2. The language code is highlighted.



3. Use the ▲▼ keys to cycle between the available languages:

- ENG (English)
- FRA (French)
- ITA (Italian)
- SCH (Simplified Chinese)
- SPA (Spanish)
- ARABIC (Arabic)
- DUT (Dutch)

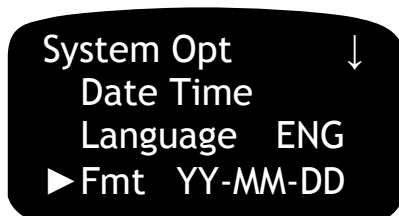
4. Press the **OK** button to confirm your selection.

If you change the setting, the DIGIgarde PLUS will not display menus and prompts in the new language until the unit is switched off and back on again.

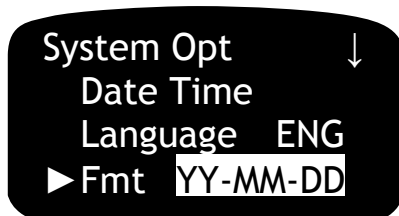
4.1.3 Date Format

To change the date format:

1. From the *Options* menu, use the ▲▼ keys to select *Fmt*. Note that the currently selected format is displayed alongside. Press the **OK** button.



2. The date format is highlighted.



3. Use the ▲▼ keys to cycle between the available date formats:

- YY-MM-DD
- YY/MM/DD
- YY.MM.DD
- MM-DD-YY
- MM/DD/YY
- MM.DD.YY
- DD-MM-YY
- DD/MM/YY
- DD.MM.YY
- YYYYMMDD

4. Press the **OK** button to confirm your selection.

4.1.4 Daylight Saving Time

To change daylight-saving time options:

1. To view further *System Opt* menu categories, use the ▼ key to scroll down past the first three categories.



2. To set the daylight saving options, select *DLST* and press the **OK** button.
The *DLST* menu is displayed.
3. To enable or disable daylight saving time, select *DLST* (the current setting is displayed alongside) and press the **OK** button.



4. Use the ▲▼ keys to cycle between the settings: *N(o)* or *Y(es)*.



5. Press the **OK** button to confirm your selection.



6. If you have enabled daylight saving time, use the *Enter DLST* and *Standard* settings to identify the beginning and end of the daylight saving time period respectively.

There are two ways to specify the start and end dates, as determined by *Date Mode*:

➤ **Mode 1 (default)**

In this mode, you specify the precise date and time. In the *Enter DLST* and *Standard* menus, DIGIgarde PLUS shows the date/time in the format:"month, day hours: minutes".

For example: 2am on the 4th September is denoted by:09 04 02 00

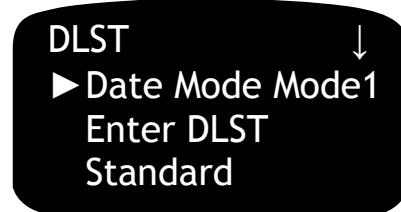
➤ **Mode 2**

In this mode, you specify the specific month and day of the week but not the precise date. A calendar month can have up to 6 weeks (although the first and

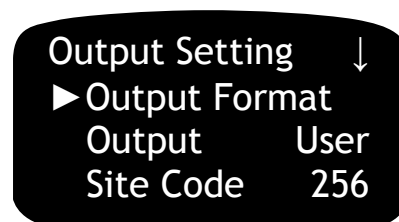
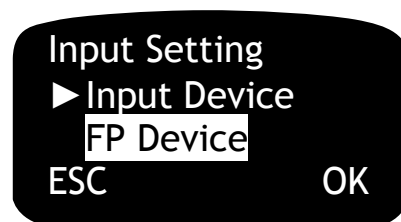
sixth will be partial weeks) so in Mode 2 you can specify, say, the first Sunday in the month by choosing week 1. The week shows the date/time as "Month - Weeks- week hours: minutes".

For example: 2am on the first Sunday in September is denoted by: 9 1 6 02:00

If you selected a Sunday in the sixth week of month, and in a particular calendar year the month only contained five weeks, DIGIgarde PLUS would assign the last Sunday of the month even if this occurred in week four.



4.1.5 Wiegand format



Input Setting

Input Setting	Use	Default
Input Device	FP Device or RF Reader	FP Device

Output Settings

Output Setting	Use	Default
Output		User
Site Code		256
Pulse Width		100
Pulse Interval		900

4.1.6 Advanced Options

The commands and sub-menus available in the *Advanced Options* menu are summarised below.

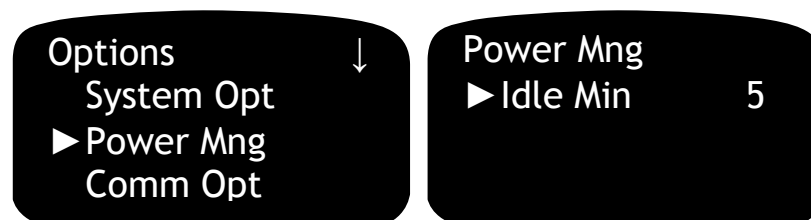


Table 10 **Advanced options**

Advanced Option	Use	Default
Reset Opts	Restore all setup options to factory default settings.	
Del AttLogs	Delete attendance logs stored on DIGIgarde PLUS.	
Clear All Data	Clear all data including all enrolled user information and attendance logs.	
Clr Admin Pri	Downgrade the Administrator's privileges to those of normal user. Note. This option is only available to users with Administrator status.	
Show Score	Choose whether to display the verification score for fingerprint matching (this may affect the verification speed).	No
Match Thr	Set the threshold level for 1:N matching	45
1:1 Thr	Set the threshold for 1:1 verification	25
Voice	Choose whether to have voice prompts and feedback	Yes
FPCard Key	Choose this option if you want the DIGIgarde PLUS to write the password to a card (6-digit PW???)	
Button Beep	Choose whether DIGIgarde PLUS beeps after each key press	Yes
Adj VOL(%)	Choose the audio volume of the DIGIgarde PLUS: H(igh, (M)edium or (L)ow	Medium
AntiPassback	Choose the anti-passback mode: None, Out, In, InOut, NoAndSa	None

4.2 Power management

Use this option to set the idle time (in minutes). If the DIGIgarde PLUS receives no keypad or fingerprint input within the Idle Time, it will go into a low power standby mode. In this mode, the screen is blank and the scanning window is unlit. If a user presses any key or places their finger on the scanning window, the DIGIgarde PLUS 'wakes' and resumes normal operation.



4.3 Communication options

The DIGIgarde PLUS fully supports RS232, RS485 and TCP/IP communications (see page 18 for connection details). Use the third option on the Options menu to set the Communication Options.

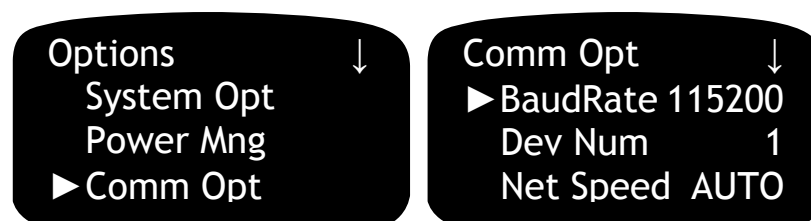


Table 11 Communication options

Communication Option	Use	Default
BaudRate	Set the baud rate for communications: 9600, 19200 38400, 57600 115200	115200
Dev Num	Choose the unit number for this DIGIgarde PLUS device: 1-255	1
Net Speed	10M-H, 100M-H, 10M-F, 100M-F, AUTO	AUTO
IP Address	Define the IP address for this unit	192.168.1.201
Netmask	Define the Net Mask for this unit	255.255.255.0
Gateway	Enter the Gateway IP address for your network.	0.0.0.0
Ethernet	Enable or disable Ethernet communications	Y
RS232	Enable or disable RS232 communications	Y
RS485	Enable or disable RS485 communications	N
COMM Key	Security key required to establish communication between unit and PC software. PC software must be configured with matching key.	0

4.4 Log options

The fourth option on the Options menu is Log Options. The DIGIgarde PLUS logs three types of data:

- Supervisor Log
- Attendance Log
- Fingerprint Alarm Log

Use the Log Options settings to determine when the unit is to indicate that the logs are reaching its internal memory capacity.

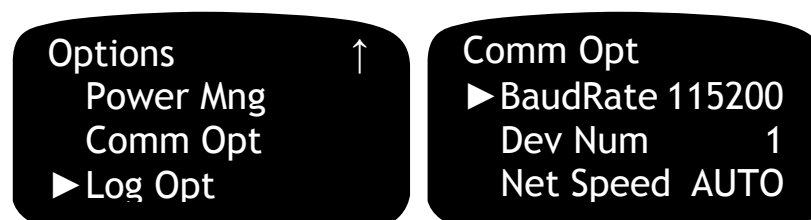


Table 12 Log options

Log Option	Use	Default
Alm SuperLog	Supervisors Log: number of remaining log entries when unit issues memory capacity warning	99
Alm AttLog	Attendance Log: number of remaining log entries when unit issues memory capacity warning	99
FRecordAlarm	Fingerprint Record Log: number of remaining log entries when unit issues memory capacity warning	99
ReCheck Min	Set the minimum period for relogging a user. If a user is verified a second time within this period, only a single log entry is recorded.	0

4.5 LED mode

The Reader LED default is set to bi-colour. The LED line is held at approximately 5V, and in normal mode will pulse to 0 Volts every 2 seconds (red LED). Upon access granted this will activate to 12 Volts (Green) for the duration of the *Lock* time (see page 48).

In ACU mode the LED is driven from the ACU.

4.6 Data out type

Wiegand or Magnetic

The reader can output the User ID with or without a site code depending upon which setting you have chosen. For connection to TDSi Access Control Panels use 37-bit Wiegand (28-bit data, 8-bit even parity, 1 bit odd parity) or Magnetic protocols.

5. Standalone Mode

As a standalone device, DIGIgarde PLUS offers advanced access control features including:

Time patterns

A time period is an allowed access timetable covering each day of the week.

Time periods can be assigned to users on an individual basis but it is more usual to apply a time period to a group of users with common working practices (for example: employees, managers, cleaners).

Examples of two time periods are shown below:

Employee time period

Sun 00:00-00:00
 Mon 08:00-19:00
 Tue 08:00-19:00
 Wed 08:00-19:00
 Thu 08:00-19:00
 Fri 08:00-19:00
 Sat 09:00-12:00

This time period allows access during Mon-Fri working hours of 8am to 7pm and on Saturday mornings. No access is permitted for this group outside these hours.

Cleaners' time period

Sun 00:00-00:00
 Mon 19:00-21:30
 Tue 19:00-21:30
 Wed 19:00-21:30
 Thu 19:00-21:30
 Fri 19:00-21:30
 Sat 00:00-00:00

This time period allows access during weekday evenings for 7 – 9.30pm. No access is permitted for this group outside these hours.

You can define up to 50 time periods and assign up to three to each group (see page 44).

Groups

To simplify the administration of users who have the same access control requirements, you can create up to five groups. A common set of time patterns and the same verification method applies to the group. However, you can choose whether each user inherits the group access options or uses their own independent time patterns and verification method.

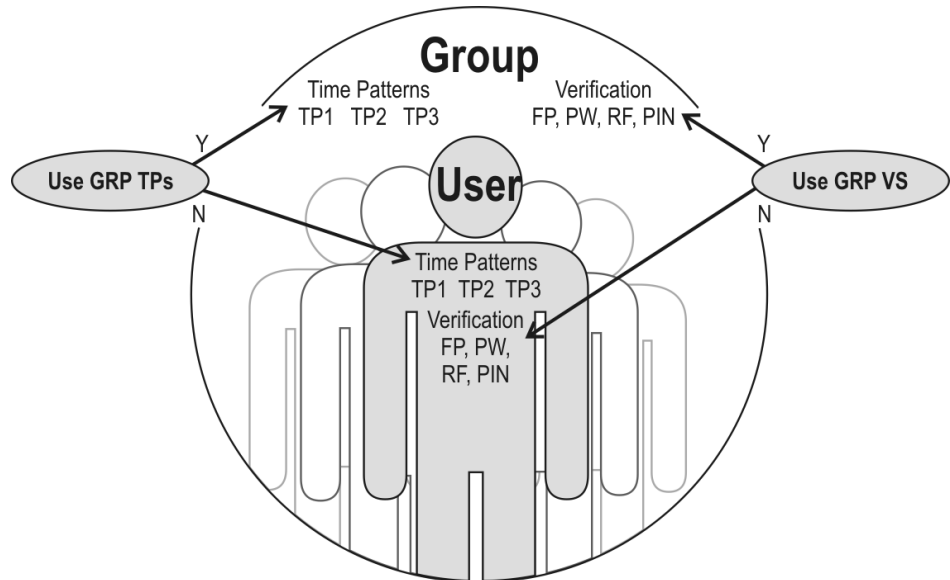


Figure 12 Access control options
Use Grp TPs and *Use GRP VS* determine whether a user is subject to their individual time patterns and verification method or those inherited from their assigned group.

Access combinations

In some circumstances, you may want to restrict access to combinations of users. For example, you may want a manager present when an employee accesses an area. In such cases, you can set up an access combination with both the employee and manager user groups. The door can then only be opened if a member of the managers' group and a member of the employees' group pass verification.

If the open door combination contains only one group, it indicates that the door is opened when any of the users in this group pass verification. If the open door combination contains two or more groups, the door is opened only after a member of each group has passed verification.

Access combinations:

Comb 1	12
Comb 2	1

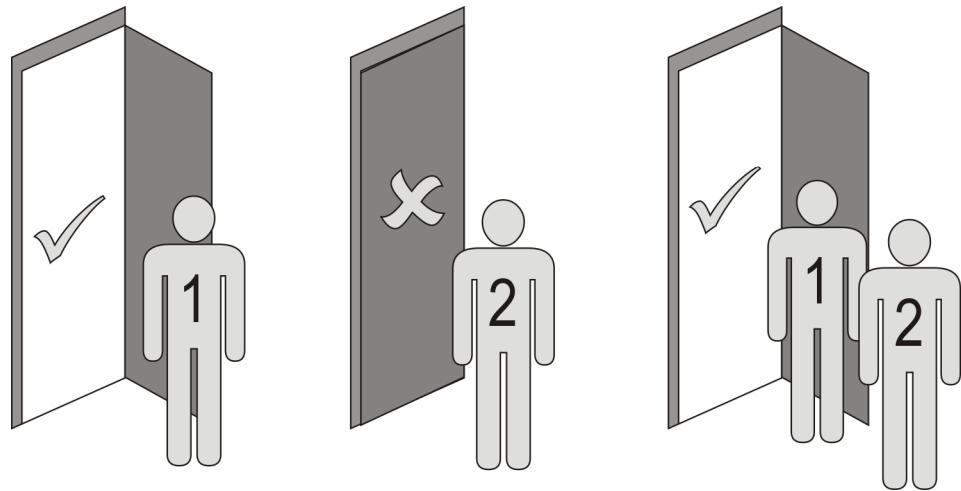
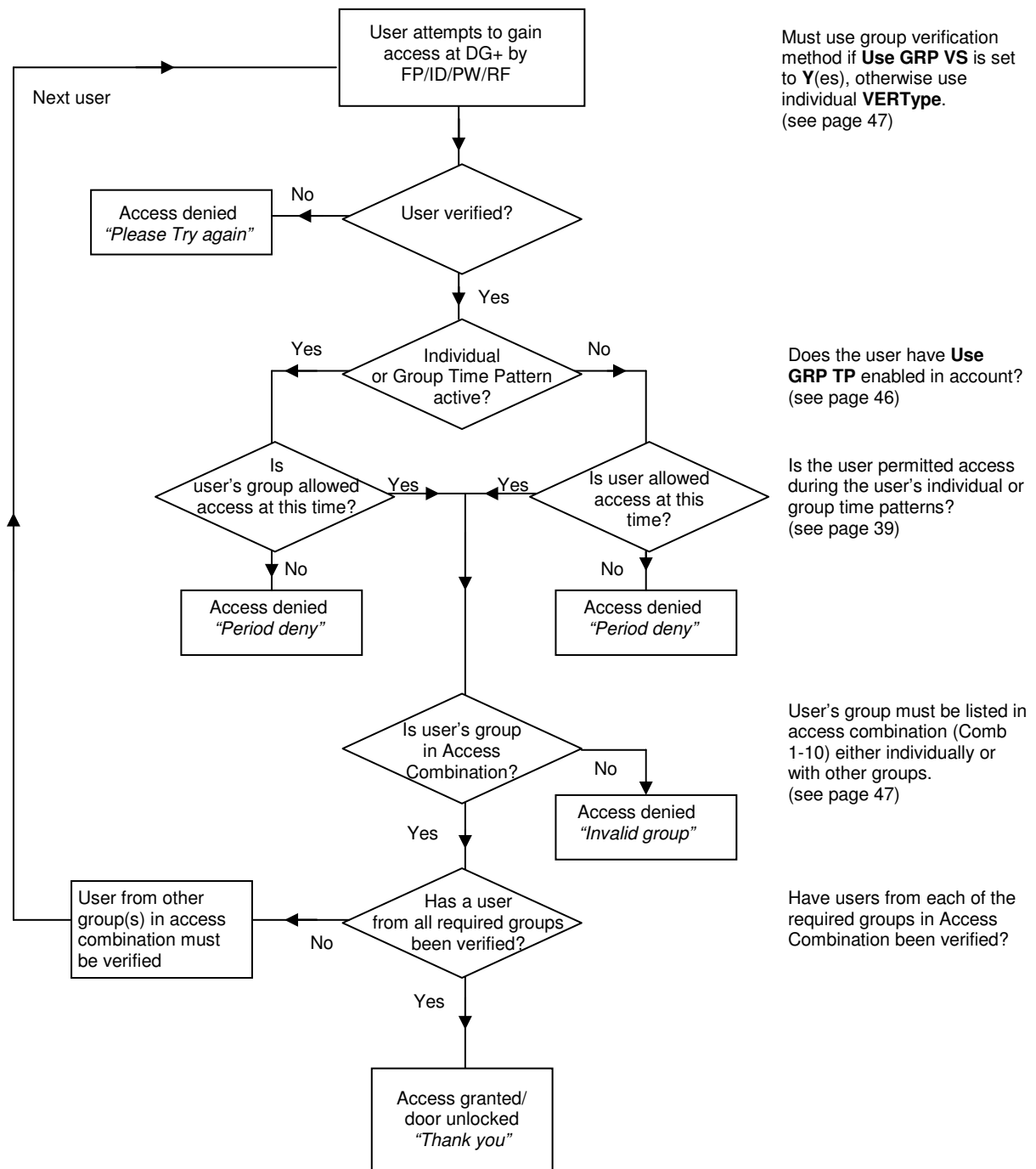


Figure 13 Example of Access combination use
With combinations of 1 & 12, members of user group 1 can gain access but users of group 2 must be verified in combination with a member of group 1.

Duress

You can assign fingerprints, passwords and/or User IDs to set off covert alarms in the event of a user being forced to verify access against their will. For example, a user might achieve normal verification using their index finger but indicate that they are under duress by using their thumb.

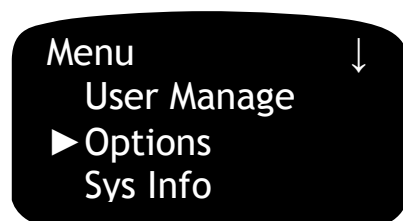
5.2 User Access Verification Flowchart



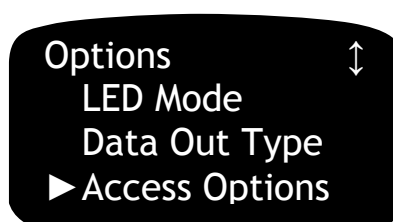
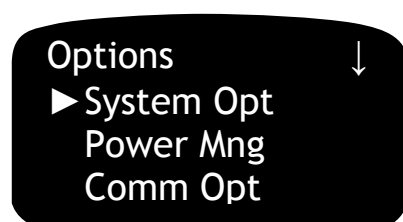
5.3 The Access Control menu

To alter any of the DIGIgarde PLUS user access settings:

1. Press the **Menu** button and, if necessary, verify your identity.
2. Press the ▼ key to select *Options*.



3. Press the **OK** button. The *Options* menu is displayed.



4. Use the ▼ key to scroll down to **Access Options**. Press the **OK** button. The Access Options menu is displayed (see Table 13).

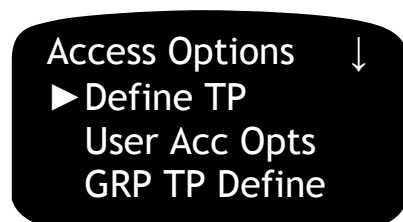


Table 13 Access Options menu

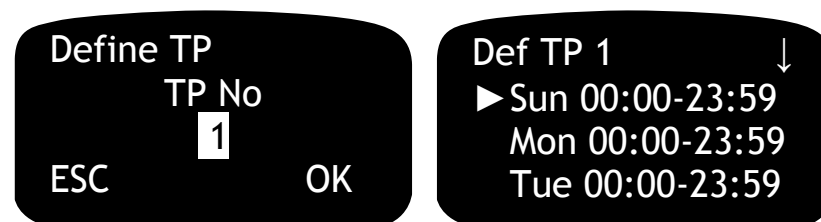
Access Options	Use	Default
Define TP	Define weekly time patterns; up to 50	1
User Acc Opts	User Account Options: assign individual users to groups, apply time patterns and verification methods.	
Grp TP Define	Define Group time period: Is used to set group unlocking time. 1-5, time period 1-50.	1
Access Comb	(Unlocking combination): define up to 10 different 5-digit unlocking combination codes (see page 47); each combination code is composed of the number and order that group users must be validated fro access.	
Lock	Time that the lock drive is powered (0-254 seconds). Set to zero to lock the door to all users.	10
Dsen.Delay	Delay time (in seconds) after the lock is powered before the DIGIgarde PLUS checks on the state of the door sensor. If the door state at this time is anything other than that set in Dsen Mode	10

	(see below) the alarm is triggered.	
Dsen.Mode	Normal state of door: none (no sensor connected), normally open (NO) or normal close (NC). DIGIgarde PLUS checks (after the DSen Delay – see above) that the door is restored to its normal state after access has been granted to a verified user.	NO
Alarm Sound	Enable or disable the unit's internal alarm.	Off
AlarmSoundTime	Set the time of the door sensor alarm	0
Duress Options	Set Duress options (see below). These settings allow you to assign fingerprints, passwords and/or User IDs to set off alarm conditions in the event of a user being forced to verify access against their will.	
ALARM CNT	Set the maximum number of consecutive failed user verification attempts before an alarm is issued: 0-99. 0: alarm off, no alarm after failed attempts.	0
GroupVerType	Assign a verification method to each of the 5 groups. Each group can have specific verification requirements, for example, fingerprint only, fingerprint and password (see page 4 for a full list of the options).	FP/PW/RF
Card Type	FPCard or Card	FPCard

5.4 Defining time patterns

A time pattern determines when a user or a group is able to gain access using their verification details (see page 39). Outside the defined hours of the time period, no access is permitted.

By default, TP1 is applied to all users and groups; initially TP1 allows access at all times.



To set up a time pattern:

1. From the Access Options menu, select **Define TP**.
2. Type the number of the Time Period (**TP No**) you want to edit. You can define up to 50 time patterns.
3. Use the **▲▼** keys to select the day you want to edit. Press the **OK** button.
4. Use the **▲▼** keys to scroll through the time definitions altering the hours and minutes as necessary.
5. Press the **OK** button to save your changes for each day. Repeat the process for the other days in the period.
6. Press the **ESC** button when you have finished.

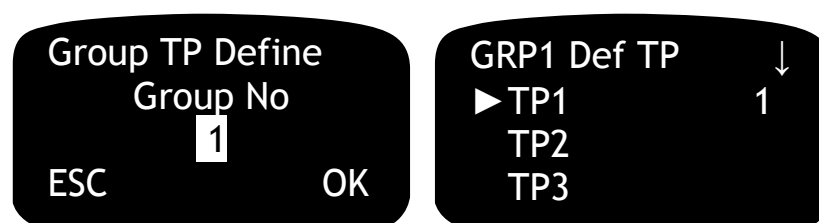
7. Press the **OK** button to confirm your changes and save the time period.
8. Define time patterns for each day of the week.

Up to 50 time patterns can be created and each time pattern can be assigned to individual users or groups.

5.4.1 Assigning a Time Pattern to a Group

1. Back in the *Access Options* menu, use the **▼** key to select **Grp TP Define**. Press the **OK** key.
2. Use the **▲▼** keys to select the number of the group (1-5). Press **OK**.
3. To edit the first time pattern (TP1 - assigned to time pattern 1 by default). Press **OK**.
4. Use the **▲▼** keys to select the required time pattern. Press **OK**.
5. If required, repeat the procedure for **TP2** and **TP3**.
6. Press **ESC**, and when prompted to save the settings, press **OK**.

The *Access Options* menu is displayed.



5.4.2 Assigning a Time Pattern to a User

By default, a user inherits the time patterns of their group but it is possible to set up independent user-specific time patterns. These options are set in the *User Access Options* menu (see below).

5.5 User Access Options

User Access Options allow you to:

- Assign a user to a group.
- Apply group or individual time patterns.
- Apply the group or an independent verification method.

5.5.1 Selecting the User

From the *Access Options* menu

1. Select **User Acc Opts**. Press the **OK** button.
2. Enter the user's ID. Press the **OK** button. The *User Options* menu is displayed.

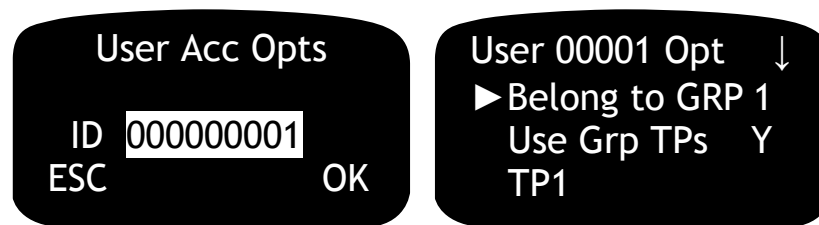


Table 14 User Access Options menu

Access Control Option	Use	Default
Belong to GRP	Assign an individual user to a Group.	1
Use Grp TPs*	Choose whether to apply time patterns from the user's assigned group (Y/N). If you select N(o), the individual's time patterns remain active even though the user is a member of a group with potentially different access time patterns.	Y
TP1	Time patterns active for this user. Use GRP TPs and the individual TP settings are linked. If you have enabled Use Grp TPs , TP1,2&3 show the numbers of the time patterns assigned to the user's group. If you subsequently edit any of these fields, Use GRP TPs is automatically disabled.	1
TP2		
TP3		
VERType	Select a verification process for this user (see page x). If Use Grp VS is enabled, this setting is ignored and the group's verification process is required.	FP/PW/RF
Use Grp VS	Choose whether to use the verification process specified for the group.	Y

5.5.2 Assigning a user to a group

By default, each new user is enrolled into group 1. If you want to assign the user to a different group:

1. Select the **Belong to GRP** option.
2. Press the **OK** button.
3. Use the **▲▼** keys to select the number (1-5) of the required group.

Now choose the user's access options: their time patterns and verification method. By default, a user inherits the time patterns and verification method assigned to the group. If preferred, you can apply user-specific time patterns and an independent verification method instead. These options are described in the next two sections.

5.5.3 Setting a user's time patterns

Having assigned the user to a group, decide if you want the user to inherit the group's time patterns or assign custom time patterns (see below).

By default, a new user inherits the time patterns of their assigned group. If you want to apply custom time patterns:

1. Select the **Use Grp TPs** option. Press the **OK** key.
2. Use the **▲** or **▼** key to change the setting to **N**. Press **OK**.

3. Use the ▼ key to select TP1. Press **OK**.
4. Use the ▲ ▼ keys to select the required time pattern. Press **OK**.
5. Repeat for TP2 and TP3.
6. Press **ESC**, and when prompted to save the settings, press **OK**.

Restoring Group Time Patterns

If you want to restore group time patterns to a user, simply change **Use Grp TPs** to **Y**. DIGIgarde PLUS automatically changes the time patterns to match those of the group.

5.5.4 Choosing a User's Verification Method

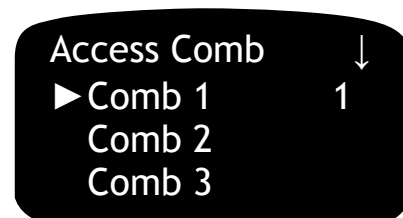
By default, a new user inherits the verification method of their assigned group. If you want to apply an individual verification method:

1. Select the **Use Grp VS** option. Press the **OK** key.
2. Use the ▲ or ▼ key to change the setting to **N**. Press **OK**.
3. Use the ▲ key to select **VERType**. Press **OK**.
4. Use the ▲ ▼ keys to select the required verification method (see page 4). Press **OK**.
5. Press **ESC**, and when prompted to save the settings, press **OK**.

Restoring Group Verification

If you want to restore the group verification method to a user, simply change **Use Grp VS** to **Y**.

5.6 Access combinations



To define an Access Combination:

1. From the *Access Options* menu, select **Access Comb**.
2. You can create up to ten access combinations. Use the ▲ ▼ keys to select the combination (Comb 1 to Comb 10). Press the **OK** button.
3. Type a 5-digit code representing the groups required for verification with this combination. For example, a combination of "12" requires that members of groups 1&2 need to pass verification to gain access.
4. Press **ESC** to save your settings and return to the *Access Options* menu.



NOTE. An access combination requires that a member of each of the specified groups passes verification. This will not occur if a user is attempting to gain access outside their valid group operating time period.

5.7 Lock and door sense

The operation of a door lock, the sensing of the door state and the triggering of an alarm if the door is not in the expected position are set by the following five options in the Advanced Options menu (see page 36):

Table 15 Lock and door sense settings

Setting	Use
Lock	Time that the lock drive is powered (0-254 seconds). Set to zero to lock the door to all users.
Dsen.Delay	Delay time (in seconds) after the lock is powered before the DIGIgarde PLUS checks on the state of the door sensor. If the door state at this time is anything other than that set in Dsen Mode (see below) the alarm is triggered.
Dsen.Mode	Normal state of door: none (no sensor connected), normally open (NO) or normal close (NC). DIGIgarde PLUS checks (after the DSen Delay – see above) that the door is restored to its normal state after access has been granted to a verified user.
Alarm Sound	Whether the alarm is triggered if the door is not in its expected position according to the Dsen.Mode setting. Default setting is <i>Off</i>
AlarmSoundTime	Set the time (seconds) of the door sensor alarm. Default setting: 0.

Example:

Lock: 10s
Dsen Delay: 15s
Dsen Mode: NC
Alarm Sound: On
AlarmSoundTime: 15s

When a user is validated, the door lock is opened for 10s. If the door is not closed 15s after validation, the unit triggers an alarm. The alarm sounds for 15s.

5.8 Alarm

The alarm connections (see page 16) are suitable for...

The Alarm is triggered if:

- The Door Sensor detects that the door is not in its expected state after a user has been verified (see page 48)
- The Alarm Count is exceeded
After a specified number of failed verification attempts by a user (see page 43).
- A Duress fingerprint or password is verified (see page 50).
- A user presses the Help ID (see page 50).

5.8.1 Resetting the alarm

If the alarm is triggered, an additional option is displayed on the main menu:



NOTE. DIGIgarde PLUS is equipped with an anti-tamper mechanism triggered if the unit is removed from its back plate while power is applied (see page 9). If this occurs, the screen displays the message "SYSTEM BROKEN".

5.9 Defining Duress options

Duress settings allow you to assign fingerprints, passwords and/or User IDs to set off covert alarms in the event of a user being forced to verify access against their will.

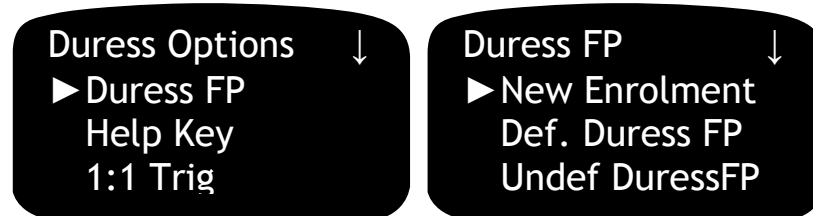


Table 16 Duress Options

Duress Option	Use	Default
Duress FP	Manage duress fingerprint enrolment for new or existing users.	
Help Key	Assign the fingerprint recorded under Duress FP as a Help key. When enabled, verification of the fingerprint will trigger the alarm.	N
1:1 Trig	Choose whether the alarm should be triggered when the user enters their ID before fingerprint verification.	N
1:N Trig	Choose whether the alarm should be triggered when the user does not enter their ID before fingerprint verification.	N
Pwd Trig	Choose whether the alarm should be triggered when the user enters their password.	N
Alarm Delay	Delay the triggering of the alarm when a user verifies a duress fingerprint or password (0-255 seconds)	10

Example:

1:1 Trig: N
1:N Trig: Y
Pwd Trig: N
Alarm Delay: 60

The duress alarm is triggered if a user verifies their fingerprint without firstly entering their ID. The alarm is set off 60s later.

Assigning the Duress FP

There are two options to set duress fingerprints:

- **New Enrolment**
Define a new user account for duress fingerprint and record the fingerprint template as described on page **Error! Bookmark not defined..**
- **Def. Duress FP**
Select an existing enrolled user and fingerprint for the duress fingerprint.

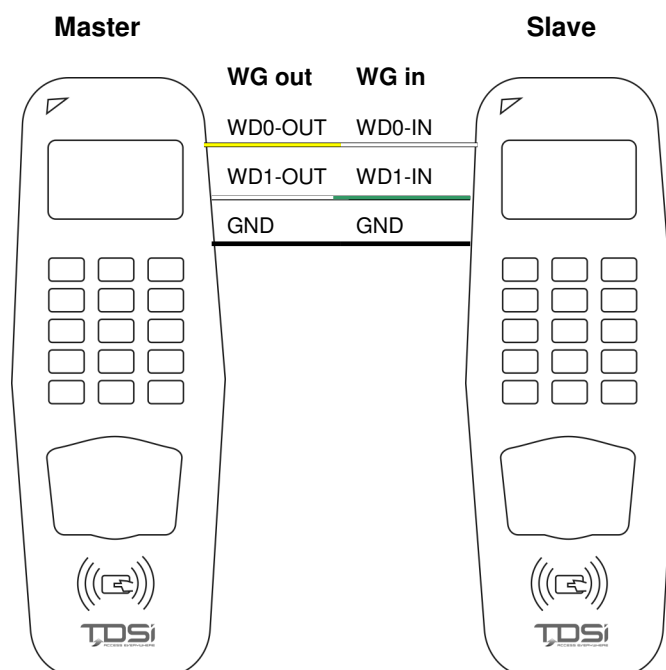
Canceling Duress fingerprints

There are two options to cancel the assignment of duress fingerprints:

- **Undef Duress FP**
Select a specific user ID and remove the duress assignment from one of its fingerprints
- **Undef All**
Remove Duress assignments from all user accounts.

5.10 Anti Passback

5.10.1 Connection



5.10.2 Set up

Master	Slave
Wiegand input	Wiegand output
Menu > Options > System Opt > Wiegand > Input Setting > <i>FP Device</i>	Menu > Options > System Opt > Wiegand > Output Setting > Output Format > <i>WG26 without ID</i>
AntiPassBack setting	
Menu > Options > System Opt > Adv Option > AntiPassback > In/Out/InOut/NoAndSa	Menu > Options > System Opt > Adv Option > AntiPassback > In/Out/InOut/NoAndSa
-	

Users must be enrolled on both master and slave units under the same user ID.

5.10.3 Use

The primary purpose of anti-passback is to prevent a person from gaining access to a restricted area by using the legitimate validation information of another registered user. For example, having been validated and gained access, a user may pass their smart card to a second person so that they also may enter the area.

With the In or InOut anti-passback modes enabled, the DIGIgarde PLUS will not allow access to a “user” unless the system has recorded that the user has previously exited the area.

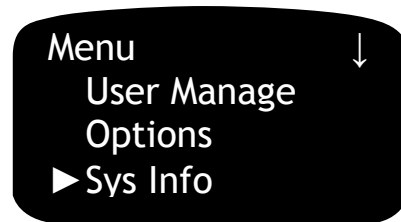
Anti-passback can also be set up to identify users who ‘tailgate’ other users into an area, thus avoiding validation and attendance logging. With the Out or InOut anti-passback modes enabled, the DIGIgarde PLUS will record incidents when a user has left the restricted area without having a previously validated record of admittance.

6. System Information

The **Sys Info** menu contains information about enrolled users, logged data and memory allocation. It contains two sub menus: **Device Info** and **Free Space Info**.

To view the Sys Info menu:

1. Press the **Menu** button and, if necessary, verify your identity.
2. Press the ▼ key twice to select *Sys Info*.



3. Press the **OK** button.

6.1 Sys Info menu

Options and settings on the Sys Info menu are summarised in the following table.

Table 17 Sys Info options

Menu option	Purpose
User Cnt	User count Number of enrolled users
FP Cnt	Fingerprint count The total amount of fingerprints
Att log	Attendance log The number of stored attendance records
Fail Record	Number of failed verifications
Admin Cnt	Administrator count Number of enrolled administrators
Pwd User	Password user Number of enrolled users verifying by password.
S Logs	Super administrator's logs Activity of administrator
Free space info	Free space information Sub menu listing remaining memory capacity for logs (see Table 19).
Dev Info	Device Information Sub-menu listing device information (see below).

6.2 Device Info menu

Options and settings on the Device Info menu are summarised in the following table.

Table 18 Device Info settings

Menu option	Purpose
FPCnt (100)	Fingerprint Count Capacity of the device for storing fingerprint templates (in hundreds); default 80 (8000)
AttLog (10k)	Attendance Log Capacity of the device for storing attendance logs (10,000s), default 5 (50,000)
S Logs	S Logs Capacity of the device for storing s logs; default 4096.
Manu Time	Manufacture Time Date and time of manufacture
Serial Num	Serial Number of device
Vendor	This device's manufacturer: TDSi
Device Name	This device's name: DIGIgarde PLUS
Alg Version	Algorithm version number: V10
Firmware Ver	Firmware version number
View MAC	MAC Address
MCU Version	MCU version

6.3 Free Space Info menu

Options and settings on the Free Space Info menu are summarised in the following table.

Table 19 Free Space Info settings

Menu option	Purpose
FP Cnt	Remaining capacity of the device for storing fingerprint templates
Att Log	Remaining capacity for storing attendance logs
Fail Record	Remaining capacity for storing information about failed verification attempts
S Logs	Remaining capacity for storing S Logs

7. Maintenance

From time to time, the surface of optical sensor, the keypad and display window may need to be cleaned.

7.1 Cleaning the Keypad and Screen

Clean the keypad and screen when visibly dirty and hard to read. To clean the keypad and screen, use a soft cloth and wipe dry.

7.2 Cleaning the Optical Sensor

Do not over-clean the sensor; it is designed to work outside when greasy or mildly dirty. However, do clean if the sensor if its performance is affected.

Clean the optical sensor as follows:

1. Switch off the DIGIgarde PLUS.
2. Blow on the surface of the sensor to clean off any loose particles.
3. Use adhesive tape to clean the surface of the optical sensor.
4. Wipe with a non-abrasive, soft, dry cloth. Be careful not to scratch the surface of the sensor. If there are lint particles on the sensor surface, blow them off when the sensor is dry.

Caution: Do not use any detergents or other cleaners.

*This page
intentionally blank*

8. Troubleshooting

8.1 How to reset language back to English

1. Ensure that the display is showing the time and date. If not, press the **ESC** key until it does.
2. Press the menu button once to display the menu.
3. Press the down arrow once (to select Options) and press **OK**.
4. Press **OK** to select *System Options*.
5. Press the down arrow once to select language and press **OK**.
6. Press the down arrow until *ENG* is displayed and press **OK**.
7. Press **ESC** and then **OK** to save the language.
8. Restart the reader.

8.2 How to reset the unit

If you lock yourself out of the menu you can get back in using an override method. Please refer to the SDK manual for details.

8.3 How to clear admin privileges

Please refer to the SDK manual for details.

8.4 When fingerprint verification fails

In some circumstances fingerprint verification fails because of the poor quality of the enrolled fingerprint. The fingerprint may have been smoothed by rubbing (such as sanding) or be subject to peeling skin through burns, disease or chemical damage.

When enrolling a user ensure that the best fingerprint is picked and in cases where these problems may occur, enrol several fingerprints. 1:1 matching may be more effective (see page 3). In extreme cases, chose a password verification method for the user.

8.5 Communication failures

There can be many reasons for communication problems:

- ✦ The communication port configuration is not correct. The configured communication port is not the COM port which is actually used.

- The baud rate between the computer communication port and the DIGIgarde PLUS are different.
- DIGIgarde PLUS is not connected to a power source or the computer.
- DIGIgarde PLUS has not completed its startup procedure.
- The serial number of a linked terminal is not correct.
- There is a problem with a data line or converter.
- The computer COM port is broken. Try testing it with another device.

8.6 Display shows “Please try again” when no finger id presented for verification

After prolonged use, the surface of the fingerprint sensor may become dirty or scratched. The DIGIgarde PLUS may sense the dirt and scratches as a fingerprint and attempt verification. Alternatively, a connecting cable may be loose or there could be an internal problem.

Clean the sensor window with some adhesive tape and a soft cloth (see page 55). Check all connections.

If the problem remains, please contact your supplier.

9. Appendices

9.1 Menu structure

User Manage

- | - Enrol User
 - | - Enrol FP
 - | - Enrol Pwd
 - | - FP & Pwd
- | - FPCard Mgr
 - | - Enrol FPCard
 - | - Create FPCard
 - | - Reg FPCard
 - | - Unreg FPCard
 - | - Empty FPCard
 - | - Dump FPCard
 - | - Move To FPCard
- | - Enrol Admin
 - | - Enrol FP
 - | - Enrol Pwd
 - | - FP & Pwd
- | - Delete

Options

- | - System Options
 - | - Date Time
 - | - Language
 - | - Fmt
 - | - DLST
 - | - Wiegand
 - | - Adv Option
 - | - Reset opts
 - | - Del Att logs
 - | - Clear all data
 - | - Clear admin privileges
 - | - Show score
 - | - Match threshold
 - | - 1:1 threshold
 - | - voice
 - | - FP card key
 - | - button beep
 - | - Adj vol
 - | - antipassback
- | - Power Mng
 - | - Idle Min
- | - Comm Opt

- ```

| - BaudRate
| - Device Num
| - DHCP
| - Net Speed
| - IP Addr
| - NetMask
| - Gateway
| - Ethernet
| - RS232
| - RS485
| - COMM Key
- Log Opt
 | - Alm SuperLog
 | - Alm AttLog
 | - FRecordAlarm
 | - ReCheck Min
- LED Mode
 | - Stand-alone
 | - Controller
- Data Out Type
 | - Wiegand
 | - Magnetic
- Access Options
 | - Define TP

 | - User Acc Options

 | - Belong to group
 | - Use Grp TPs
 | - 2. TP1
 | - 3. TP2
 | - 4. TP3
 | - VERType
 | - Use Grp VS
 | - Group TP Define
 | - TP 1 - 5
 | - Access Comb
 | - Lock
 | - Dsen. Delay
 | - Dsen. Mode
 | - Alarm Sound
 | - AlarmSoundTime
 | - Duress Options
 | - ALARM CNT
 | - Group VerType
 | - CardType FGCard
- Auto Test
 | - Run All Test
 | - LCD Test
 | - Voice Test
 | - FP Reader

```

- | - Key Test
- | - RTC Test

## Sys Info

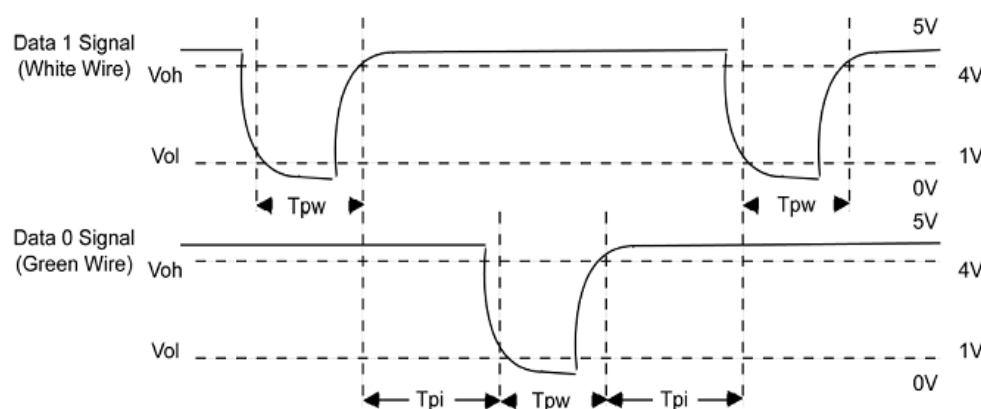
- | - User Cnt
- | - FP Cnt
- | - Att Log
- | - Fail Record
- | - Admin Cnt
- | - Pwd User
- | - S Logs
- | - Free Space Info
  - | - FP Cnt
  - | - Att Log
  - | - Fail Record
  - | - S Logs
- | - Dev Info
  - | - FPCnt(100)
  - | - AttLog(10k)
  - | - S Logs
  - | - Manu Time
  - | - Serial Num
  - | - Vendor
  - | - Device Name
  - | - Alg Version
  - | - Firmware Ver
  - | - View Mac
  - | - MCU Version

## 9.2 Wiegand format

The figure below displays the timing pattern for data bits sent by the reader to the access control panel. This timing pattern falls within the Wiegand guidelines as proscribed by the SIA's Access Control Standard Protocol for the 26-Bit Wiegand Reader Interface (a Pulse Width time between 20µs and 100µs, and a Pulse Interval time between 200µs and 20ms). The Data 1 and Data 0 signals are held at logic high level (above the Voh level) until the reader is ready to send a data stream. The reader places data as asynchronous low-going pulses (below the Vol level) on the Data 1 or Data 0 lines to transmit the data stream to the access control panel. The Data 1 and Data 0 pulses will not overlap or occur simultaneously. Table 1 provides the minimum and maximum allowable pulse width times (the duration of a pulse) and pulse interval times (the time between pulses),

**Table 20 Wiegand pulse characteristics**

| Symbol | Description         | Reader typical Time |
|--------|---------------------|---------------------|
| Tpw    | Pulse Width Time    | 100µm               |
| Tpi    | Pulse interval time | 1ms                 |



**Figure: Time**

### 9.2.1 Wiegand format

F Series Fingerprint Access Control Wiegand format is a general Access Control protocol.

## 9.2.2 26-bit Wiegand format

The composition of the open de facto industry standard 26 Bit Wiegand format contains 8 bits for the facility code field and 16 bits for the ID number field. Mathematically these 8 facility code bits allow for a total of just 256 (0 to 255) facility codes, while the 16 Id number bits allow for a total of only 65,536 (0 to 65,535) individual ID's within each facility code.

**Table 21 26-bit Wiegand field definition**

| Field                        | Purpose                                                        |
|------------------------------|----------------------------------------------------------------|
| <b>EP</b>                    | Even parity bit, over bits 1 to 13.                            |
| <b>FC</b><br>(bit 2-bit 9)   | Facility code (0-255),<br>bit 2 is MSB ( most significant bit) |
| <b>CC</b><br>(bit 10-bit 25) | Card code, (0-65,535)<br>bit 10 is MSB (most significant bit)  |
| <b>OP</b>                    | Odd parity bit, over bits 13 to 26                             |



Time and Data Systems International Ltd  
Unit 10 Concept Park  
Innovation Close  
Poole  
Dorset  
BH12 4QT  
UK

t: +44 (0)1202 723535  
f: +44 (0)1202 724975  
w: <http://www.tdsi.co.uk/>

Sales Enquiries: [sales@tdsi.co.uk](mailto:sales@tdsi.co.uk)  
General Enquiries: [info@tdsi.co.uk](mailto:info@tdsi.co.uk)  
Marketing Support: [marketing@tdsi.co.uk](mailto:marketing@tdsi.co.uk)  
Technical Support: [support@tdsi.co.uk](mailto:support@tdsi.co.uk)