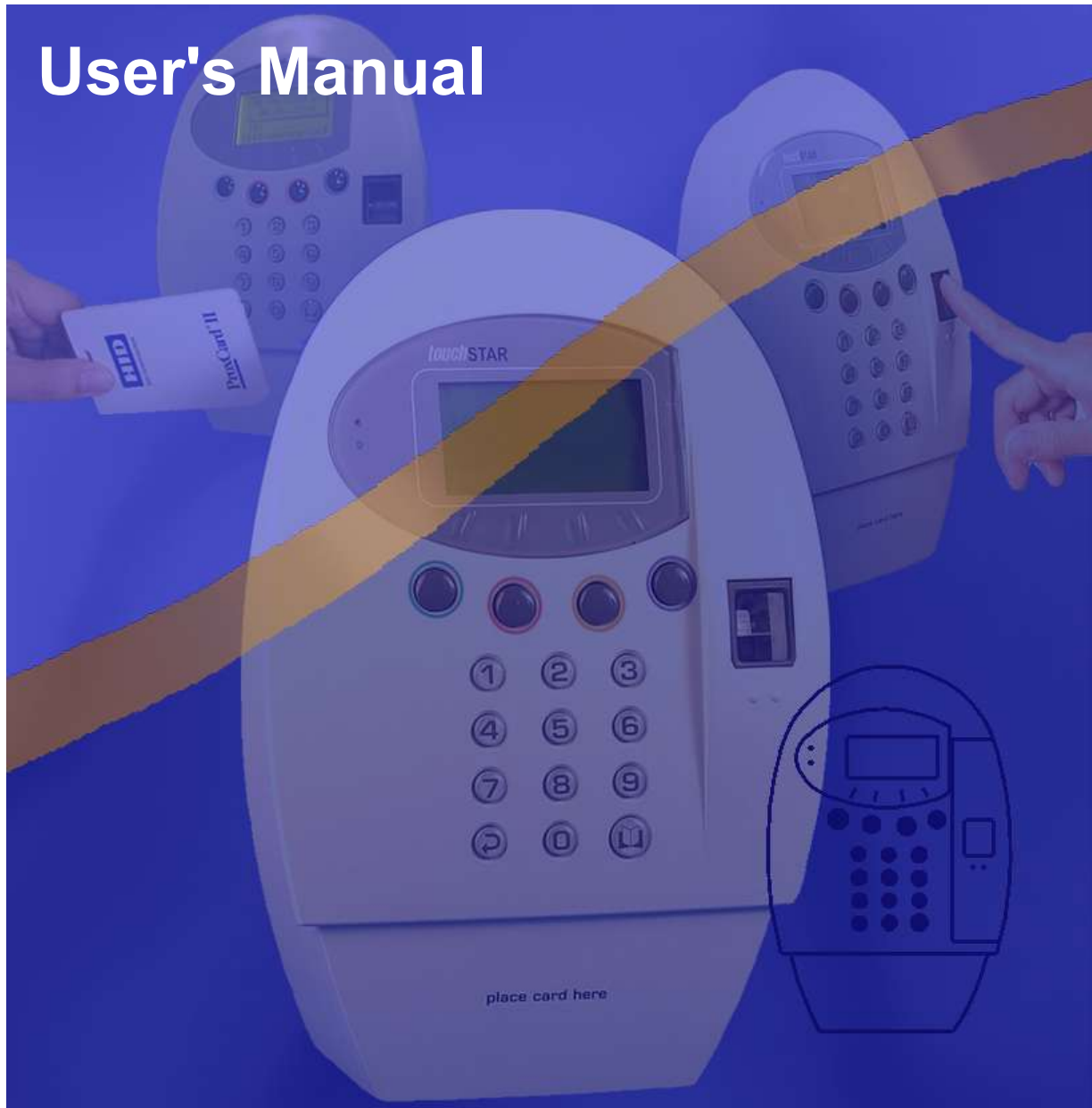


TouchStar

**Time Attendance and Door Access
Fingerprint Reader**

User's Manual



Autostar Technology

Notices :

Information in this document is subject to change without notice.

NO WARRANTY OF ANY KIND IS MADE WITH REGARD TO THIS MATERIAL INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

No liability is assumed for errors contained herein or for incidental damages in connection with the furnishing, performance, use of this material.

No part of this document may be photocopied, reproduced or transmitted in any form or by any means, electronic or mechanical, without the prior written permission of Autostar Technology Pte Ltd.

Other products and corporate names may be trademarks or registered trademarks of other companies and are only for explanation without intent to infringe.

Copyright 2005 Autostar Technology Pte Ltd, Singapore
All rights reserved.

Document Name : TouchStar User's Manual (2nd Edition)

Document Date : 18 Apr 2005

Revision 1.1

Preface

"We do not just offer a device; but a complete fingerprint identification solution."

Thank you for choosing TouchStar Fingerprint Identification System. It is not only a device that is simple to use, but it also provides a host of versatile, flexible and powerful features at the same time.

In this manual, you will learn about the features provided by the device, how to administrate the device, how to communicate with the device and how to interface it to door controllers.

How to use this manual

You can browse from start to end...

If you are reading this manual for the first time, you may like to flip through it from start to end to achieve an overall understanding.

If you are looking for specific information, use the Table of Contents to help you...

If you are looking for some specific information, you may turn to the Table of Contents to speed up your search for the relevant information.

The manual has been written in such a way that the commonly encountered procedures are described in Chapter 4 (Basic Administration), while the advanced ones are in Chapter 5 (Advanced Administration).

If you know what you want to do, you can look under one of these chapters in the Table of Contents to look for the relevant procedure. They procedures are categorized according to how they appear in the TouchStar menu.

The Table of Contents is on the next page.

To understand more about specific features, you can refer to Chapter 3 (Features). At times, more detailed information are provided under the specific procedure described found in Chapter 4 or Chapter 5.

If you are quite new to TouchStar, you may like to read Chapter 1 (Getting to Know TouchStar) and Chapter 2 (Getting Started). This should get you started on basic setup.

Table of Contents

1	Getting to Know TouchStar	1
1.1	Features.....	1
1.2	How TouchStar Works.....	2
2	Getting Started	4
2.1	Checking the Packing	4
2.2	Identifying the Parts.....	4
2.3	Applying Power.....	6
2.4	Enrolling the First Master.....	7
2.5	Communicating with TouchStar	7
3	Features	8
3.1	Authentication And Managing Authentication Properties.....	9
3.1.1	Understanding the Authentication Properties in TouchStar.....	9
3.1.2	Understanding Speed Search and One-To-Many Search.....	11
3.1.3	Understanding Multiple Fingerprint Verification.....	12
3.2	Central Administration.....	12
3.3	Timezone in TouchStar.....	13
3.4	Using the Relay in TouchStar.....	14
3.5	Logging.....	16
3.5.1	Preventing Duplicated Log Records.....	17
3.5.2	Viewing Recent Log Records.....	17
3.6	Interfacing with Door Controllers through Wiegand.....	18
3.6.1	Third Party Door Controllers.....	18
3.6.2	TouchStar Door Zone Controller.....	18
3.6.3	Waiting for an Acknowledgment Signal from External Controller to Indicate Receipt of Wiegand Sent.....	19
3.6.4	Sending Special Wiegand Code to Indicate Failed Verification.....	19
4	Basic Administration	20
4.1	Understanding and Using the User Page.....	20
4.1.1	Performing Matching at the User Page.....	21
a.	Fingerprint Matching.....	21
b.	Card Only Matching.....	23
c.	PIN Matching.....	23
4.1.2	Viewing Recent Log Records.....	24
4.1.3	Viewing TouchStar Technical Information.....	25

4.2	Understanding and Using the Master Page.....	26
4.2.1	Entering the Master Page.....	26
4.2.2	Menu Map in the Master Page.....	28
4.2.3	Navigating the Master Page (Read This).....	29
4.2.4	Inside the ENROLL Page.....	32
a.	Adding a Master.....	32
b.	Adding a User.....	33
c.	Deleting a Master.....	36
d.	Deleting a User.....	37
e.	Searching for a Master Or User.....	37
f.	Deleting all User Records from Device.....	38
4.2.5	Inside the CONFIG Page.....	39
a.	Setting the Time.....	39
b.	Setting the Date.....	40
c.	Setting the Door Control.....	41
d.	Setting the Communication Type as RS-232, RS-422, RS-485, Modem or TCP/IP.....	42
e.	Setting the Alarm.....	46
f.	Configuring the Wiegand Settings.....	48
g.	Enabling or Disabling Timezone Checking.....	50
4.2.6	Inside the LOG Page.....	51
a.	Display all the Logs.....	51
b.	Erasing all the Logs.....	52

5 Advanced Administration

53

5.1	In the Master Page.....	53
5.1.1	In the ENROLL Page.....	53
a.	Setting the Security Level and Identify Mode.....	53
b.	Allowing Device Masters to Be Enrolled as Card Only or PIN.....	54
c.	Viewing the Fingerprint Sensor's Calibration Settings.....	56
5.1.2	Inside the CONFIG Page.....	57
a.	Setting the Clock Drift Adjustment.....	57
b.	Setting the Number of ID Digits.....	58
c.	Setting the Fail Wiegand Out Option.....	59
d.	Configuring the External Input Detect.....	60
e.	Configuring the Relay Option.....	61
f.	Selecting the Language.....	65
g.	Selecting the Time Attendance Field Descriptor Set.....	66
h.	Selecting the Auxiliary Device.....	67
i.	Enabling or Disabling the Numeric Keys.....	70
j.	Displaying or Hiding the Card ID.....	71
k.	Setting the Multiple Fingerprint Verification Option.....	72
l.	Allowing Keypad Input to Replace Card Input for Fingerprint Verification.....	73
m.	Allowing Keypad Input to Replace Card Input for PIN Verification.....	74
n.	Setting the Number of PIN Digits.....	75
5.1.3	Inside the LOG Page.....	76
a.	Setting the Duplicate Check Option.....	76
b.	Enabling or Disabling Event Trace, Failed Attempts and Authentication Mode Trace Logs.....	77

6	Setting Up for Communication	78
6.1	Using RS-232.....	78
6.2	Using RS-422 and RS-485.....	80
6.2.1	RS-422.....	81
6.2.2	RS-485.....	82
6.3	Using TCP/IP.....	83
6.4	Using the Modem.....	85
6.4.1	Single TouchStar.....	86
6.4.2	Multiple TouchStar Devices.....	88
7	Setting Up for Access Control	90
7.1	Using a Third Party Door Controller.....	90
7.2	Using the TouchStar Door Zone Controller.....	91
8	Appendices	93
Appendix A	– Technical Specifications.....	93
Appendix B	– TCP/IP Subnet Mask Translation.....	94
Appendix C	– TouchStar Door Zone Controller.....	95
Appendix D	– Using the On-board Relay for Door Control.....	97
Appendix E	– ADAM 4520 RS-232 to RS-422 / 485 Interface Converter.....	99
Appendix F	– Using the ADAM-4520 in RS-422 and RS-485 Communication.....	101
Appendix G	– Testing or Troubleshooting TCP/IP Connections.....	105
Appendix H	– Log Types in TouchStar.....	107
Appendix I	– Care and Maintenance.....	111

Chapter 1

1 Getting to Know TouchStar

TouchStar is a fingerprint identification device designed for use in time attendance and access control. It is a user-friendly device which is easy to understand and convenient to use.

You can enroll your fingerprints through the device, or using the software package that comes with it. Once you have enrolled your fingerprint into the device, you will be allowed to perform fingerprint authentication at the device.

Let's take a look at some of the features provided by TouchStar, and understand how it works.

1.1 Features

Fingerprint Technology

- ❑ State-of-the-art fingerprint extraction and verification technology
- ❑ Fingerprint minutiae encryption algorithm
- ❑ Fingerprint sensor immunity to electrostatic discharges

Device

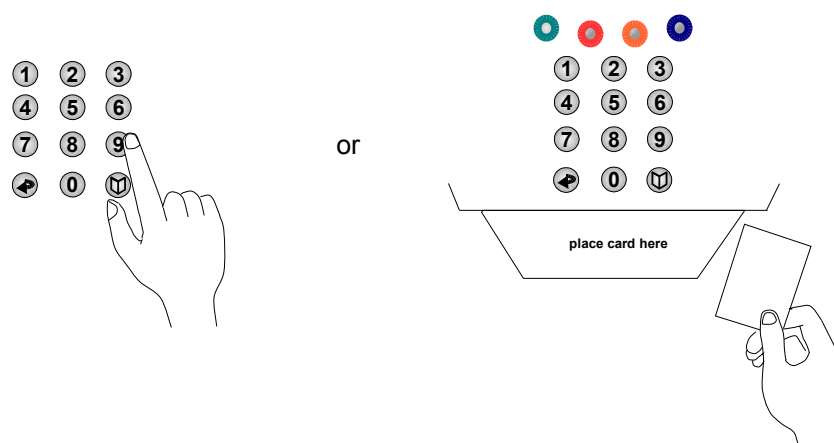
- ❑ Elegant outlook and tamper proof design
- ❑ Easy to navigate and user friendly administrator mode
- ❑ Large 128 by 64 graphic LCD with power saving LED backlight
- ❑ Each user can enroll up to 6 fingerprints using the same ID.
The device will try to look for the matching fingerprint associated with this ID.
- ❑ Supports both local and centralized enrollment
- ❑ Supports one-to-many fingerprint identification.
- ❑ Supports all common serial communication interfaces such as RS-232, RS-485, and RS-422.
- ❑ Supports Wiegand input and output interface.
- ❑ Plug-in option for Ethernet (TCP/IP) connection.
- ❑ Supports external devices like barcode reader and magnetic stripe reader
- ❑ Supports internal devices like HID and Mifare contactless reader
- ❑ Unique **Speed Search** verification, which you can just enter the trailing portion of your ID and scan your fingerprint
- ❑ Supports the check for duplicate log.
This prevents users from 'clocking in' at the device again when used as a Time Attendance device.
- ❑ Allows user to sound an externally connected bell at different timings.
- ❑ Supports Timezone control

1.2 How TouchStar Works

The following provides a brief outline of how the TouchStar device works.

TouchStar associates each user record with a User ID

Each user record is associated with a User ID. This User ID can be entered through the keypad, or it can be captured from a card scan.



Methods of providing the User ID

If you enrolled your fingerprint with a User ID that is taken from the keypad, you just need to key in the ID using the keypad during verification. Alternatively, you can scan a card bearing the same ID across the device.

On the other hand, if you enroll your fingerprint together with a User ID that is captured from a card scan, during verification, you would need, to likewise, present the card for the fingerprint authentication to take place. The presence of the card is thus as an additional authentication factor. This adds to increased security.

Whichever way you choose, TouchStar would next ask you to place your finger for verification after confirming that this ID exists.

In short, how you enroll affects how you are able to authenticate. To learn more about the authentication modes, you can refer to “**Chapter 3.1 - Authentication And Managing Authentication Properties - (page 9)**”.

TouchStar caters for exceptions

When a security system is rolled out in an organization, typically, there would be a few persons whose fingerprints are bad enough that they cannot be recognized in fingerprint recognition devices.

To cater for these exceptions, TouchStar is designed to cater for card alone access, or a combination of card and a secret PIN. By doing so, a system can be successfully implemented across all users in an organization.

Communicate with TouchStar using serial, the modem or TCP/IP

The TouchStar system supports different modes of communications. The supported serial modes are RS-232, RS-422, or RS-485. In addition, you can also communicate with the device using the modem or a network TCP/IP link.

Local enrollment and central enrollment

The TouchStar system is designed to cater for both local and central enrollment.

By local, it means that the device caters for users to enroll directly on the device.

By central, it means that the users of the device are enrolled centrally on a host PC using the central enrollment software. The enrolled fingerprint templates are then downloaded by means of a communication link to the TouchStar device.

On top of these, the fingerprint that is enrolled on the device can also be uploaded through the central enrollment software and be saved into the software.

TouchStar stores users as device masters or device users

When you are enrolling using your fingerprint, you can choose to enroll as a device master, or as a device user.

A device master is someone whose fingerprint is allowed to enter the administration mode of the device. The administration mode is akin to the programming mode where settings can be changed, as well as other device masters or users can be enrolled or deleted.

A device user, on the other hand, does not have this privilege access. You can read more about administration in “**Chapter 4 – Basic Administration (page 20)**”.

The TouchStar device can enroll a maximum of 20 masters. On top of that, each master ID can enroll up to 6 fingerprints. With many masters allowed, you can assign more than one person to administrate the devices.

Logging of transactions

Every time a user successfully verifies his fingerprint at the device, a transaction log is recorded. This log remains in the device in a round-robin flash storage. The role of the host software is to upload the log from the device to the host PC.

Logging of events

Besides the transaction logs, there is also another category of logs which is known as event logs. Event logs are recorded whenever any exceptional events happen. An example of such an event is an instance when the alarm is triggered.

Event logs are turned off by default so that they do not take up log space since they share the same space as the transaction logs.

Wiegand interface to external door controllers

TouchStar provides a Wiegand output interface to an external door controller. Wiegand signals are sent out upon a successful verification of the fingerprint so that the door controller is able to unlock the door.

Summary

This chapter should have provided you with a brief knowledge of TouchStar and how it operates. In the next chapter, we will get started on using the device.

Chapter 2

2 Getting Started

2.1 Checking the Packing

Before we shipped the unit to you, our valued customer, we have carefully inspected TouchStar both mechanically and electrically against any defects. They should be free of marks and scratches and you should expect it to be in perfect order on receipt.

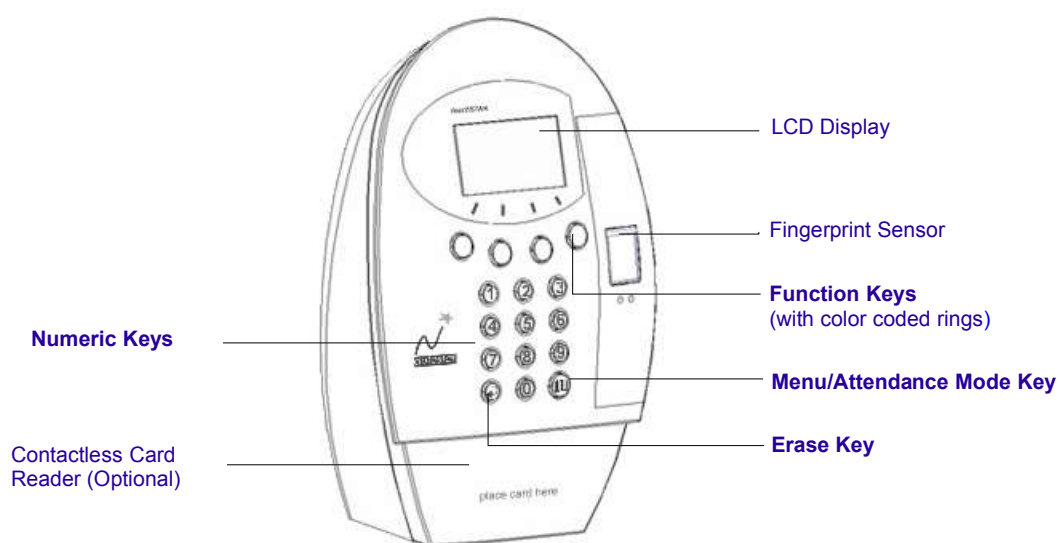
As you unpack the box, check them for signs of shipping damage (such as damaged box, scratches or dents). The following items are included in the packing box:

- Packing list
- TouchStar unit (must be wrapped in plastic bag)
- Power adapter (with a 6-way screw terminal block attached to it)
- RS-232 serial communication cable
- CDROM (software and user's manuals)
- Warranty statement and registration card

Verify the items against the packing list and inform us if there are any discrepancies immediately.

2.2 Identifying the Parts

The illustration below shows the physical parts of TouchStar. The same naming convention will be used throughout this manual.



Parts of TouchStar

LCD Display

The LCD display shows the current operation status of TouchStar.

When TouchStar powers up, the startup screen will appear for several seconds followed by the User Page. The User Page is the screen that shows the digital clock and the ID field. It is also where you would perform authentication.

To conserve energy, the LCD backlight is switched off automatically if it has been inactive for about 30 seconds. Any key presses or card scans would turn it on again.

Function Keys

The purpose of the 4 function keys are different between the User Mode and the Administration Mode.

In the User Mode, each function key is predefined for a specific operation. The function can only be activated when you press it a predefined number of times. The name of the function will not be shown on the LCD screen. The screen here is also referred to as the User Page.

In the Administrator Mode, the function keys are used to navigate and make selections. The name of the function will be shown on the bottom line of the LCD screen. The screen here is also referred to as the Master Page.

Numeric Keys

The numeric keys are used to enter your User ID or PIN when performing authentication.

Erase Key

The erase key allows you to delete (or backspace) the last digit of the User ID that was entered.

Menu Key

The menu key allows you to select the relevant mode during the authentication process. The selected mode will be written into the log record if the authentication is successful. This information can be used for payroll calculation or for tracking the movement of personnel.

Fingerprint Sensor

This is where you will place your finger for fingerprint capturing. Red light (LED source) is turned on when fingerprint capturing is active.

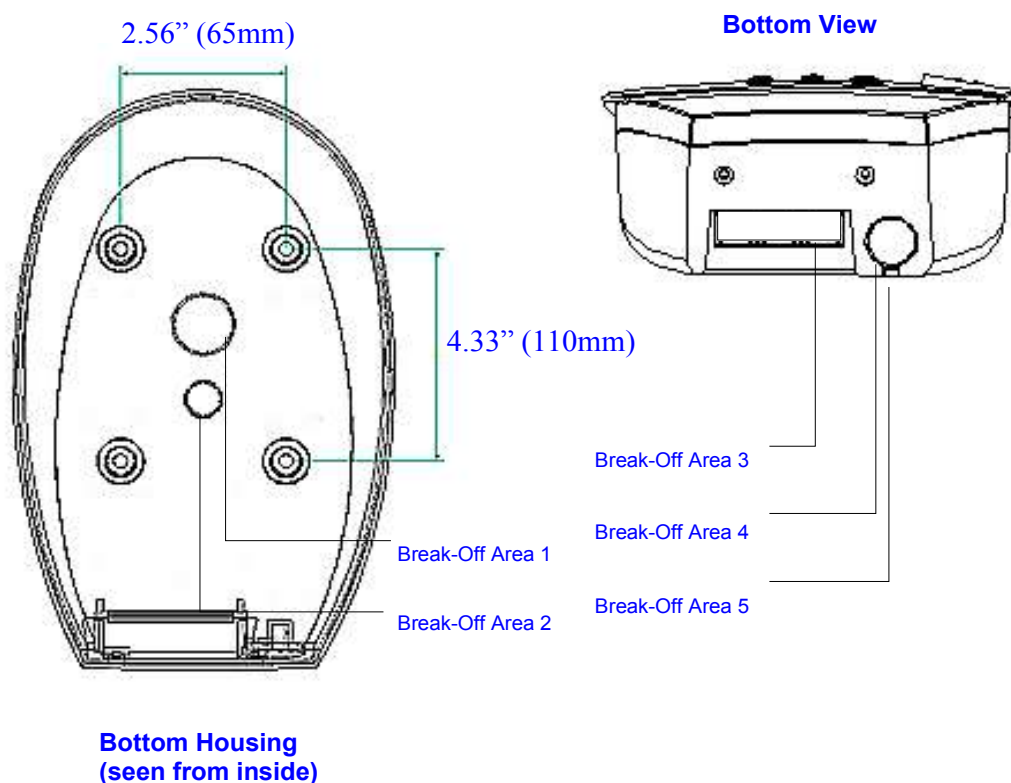
Contactless Card Reader

The contactless card reader is concealed inside the TouchStar enclosure. You can scan your contactless card if your TouchStar is fitted with a contactless card reader. To scan your contactless card, you will have to place it within a range of 50mm from the text “place card here”. Your card ID will be shown in the ID field of the User Page.

2.3 Applying Power

Remove break off area:

In order to apply power to TouchStar, one of the break off areas has to be removed to allow the power cable to pass through. Choose one of the available break off areas shown in the diagram below. A pair of cutter would be handy.



Break off areas in TouchStar

Checking the power adapter:

Warning:

Before you power on, make sure that the voltage rating of the power adapter is suitable for use in your country. If you are in doubt, please consult your local representative for advice.

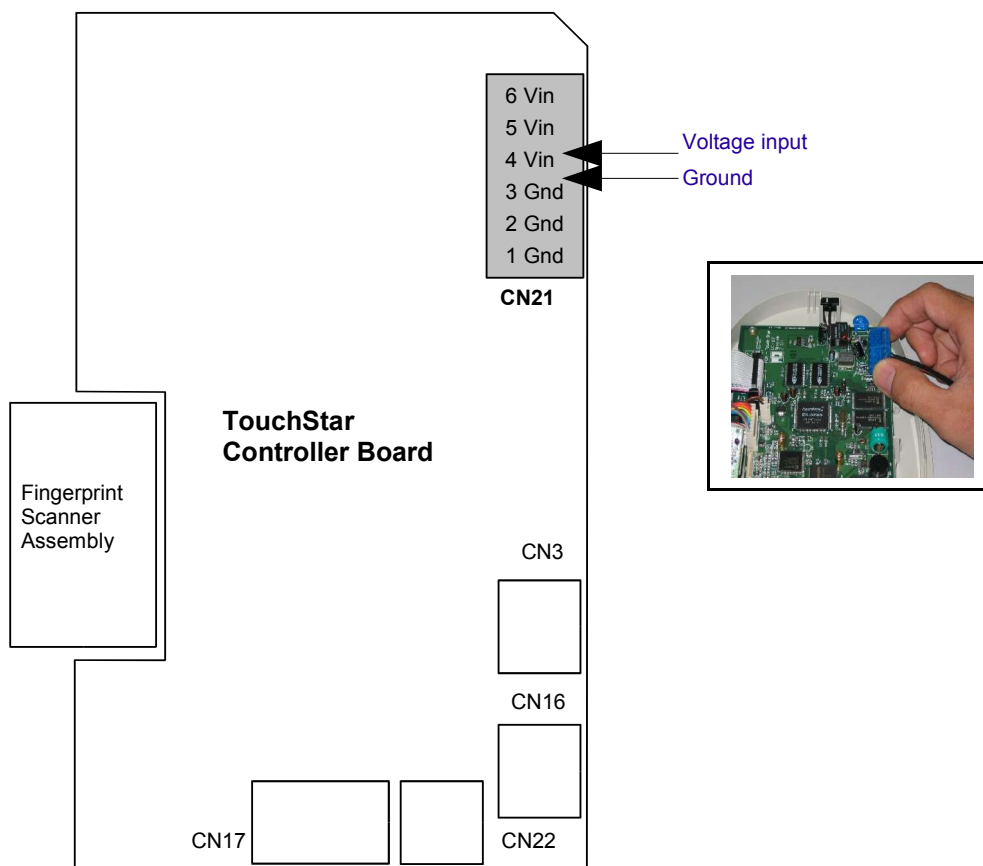
Depending on what you have ordered, you shall receive one of the power adapters as listed below:

- i. Model DV-1280-3 for 120VAC, 60Hz input and 12VDC, 1A output (UL recognized Class 2 power supply) for US and Canada.
- ii. Model DV-1280-3UP, for 230VAC, 50HZ input and 12VDC, 1A output.

If you intend to replace with other types of power adapter, make sure it is a UL recognized Class 2 power supply and the output voltage is between 12V to 24VDC rated at 1.0A. You can also refer to **"Appendix A – Technical Specifications (page 93)"** for other specifications.

Plugging in the screw terminal block for the power supply:

If you notice, the other end of the power adapter is attached to a 6-way screw terminal block. Plug in this end onto CN21 of the TouchStar controller board. Switch on the power next and observe the LCD screen of TouchStar as it powers up.



Applying power to TouchStar

2.4 Enrolling the First Master

After you have powered up the device, you may like to enroll yourself. The first user of the device automatically becomes the first device master. To enroll yourself as the first device master, please follow the procedure described in “**Chapter 4.2.4a – Adding a Master (page 32)**”.

2.5 Communicating with TouchStar

Having enrolled yourself as the first master, you may now setup TouchStar to communicate with it. TouchStar caters for various modes of communication. You can refer to “**Chapter 6 - Setting Up for Communication (page 78)**” for the type of connection required for each mode of communication. In addition, you also need to set the device with the proper menu setting. For this menu setting, please refer to “**Chapter 4.2.5d – Setting the Communication Type (page 42)**”.

Chapter 3

3 Features

In this chapter, we will look at the features provided by TouchStar. The features are grouped into categories to help you to look for information quickly. The table below shows the various categories.

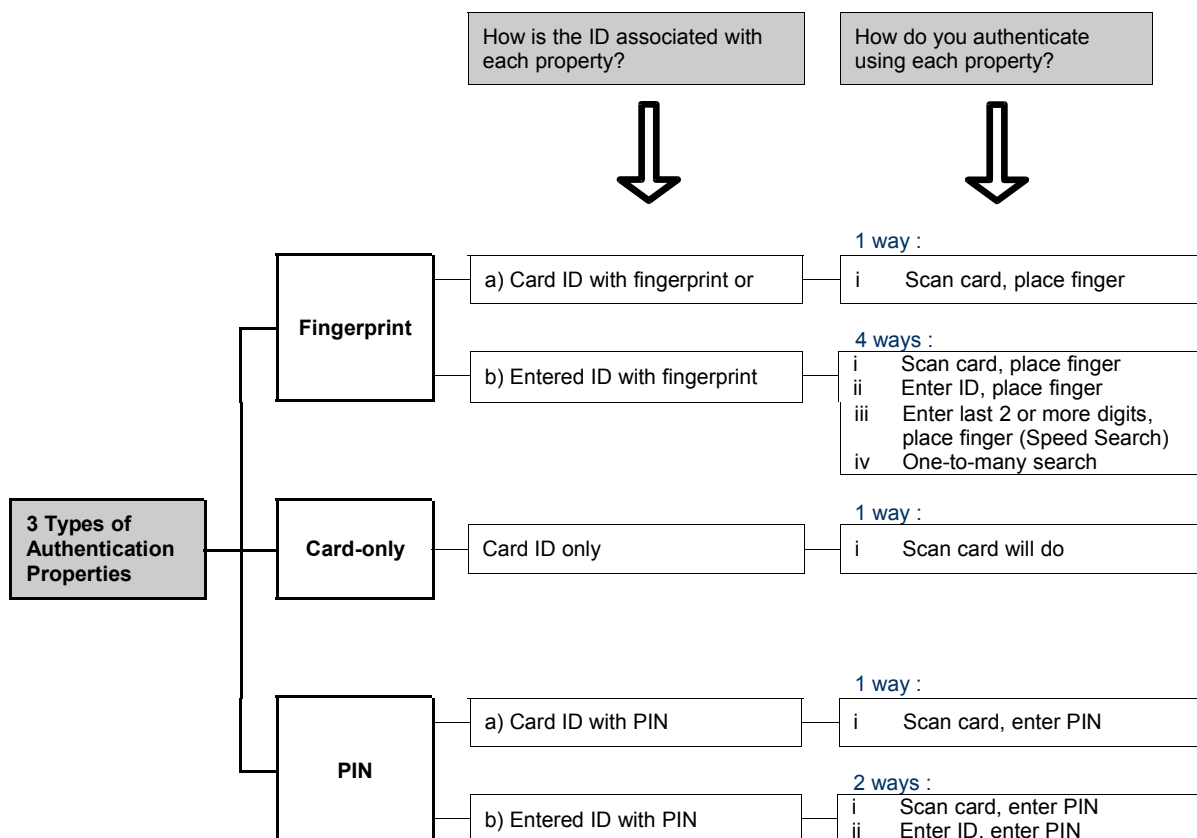
Table of Feature in TouchStar:

	Group	Section
1	Authentication and managing authentication properties <ul style="list-style-type: none"> • Enrollment and verification with fingerprint, card only or PIN • Speed Search and one-to-many search • Multiple fingerprints verification 	3.1
2	Central administration	3.2
3	Using Timezone in TouchStar <ul style="list-style-type: none"> • User's timezone control (Personnel Schedule) • Automatic door open and close schedule (Door Schedule) 	3.3
4	Using the relay in TouchStar <ul style="list-style-type: none"> • For indicating a successful authentication with an external bell or light • For sounding a bell at fixed times 	3.4
5	Logging <ul style="list-style-type: none"> • Transaction, trace events, failed attempts and authentication mode trace logs • Checking for a duplicated transaction • Displaying recent log records 	3.5
6	Interfacing with door controllers via Wiegand <ul style="list-style-type: none"> • Third party controllers • TouchStar Door Zone Controller • Waiting for an acknowledgment signal from controller to indicate receipt of Wiegand sent • Sending special Wiegand code to indicate failed verification 	3.6

3.1 Authentication And Managing Authentication Properties

3.1.1 Understanding the Authentication Properties in TouchStar

Authentication properties refer to the type of profile that you enroll yourself with. Fingerprint is not the only available authentication property in TouchStar. The other two types of authentication properties are card-only and card or ID with a secret PIN. The chart below illustrates the 3 types of authentication properties.



Authentication properties in TouchStar

The User ID can be taken from keypad input or card input

The chart also illustrates how is the User ID associated with each property. The User ID can be taken from the keypad input, or it can be captured from a card.

If the User ID is captured from a card during enrollment, the card will be treated as an additional authentication factor. During subsequent authentication, the card will always be required. Let us look at the details for each type of authentication property.

Authenticating yourself using each of the authentication properties

a) Doing a fingerprint authentication:

If you enroll yourself using fingerprint, the User ID that is associated with this fingerprint can either come from the keypad input or a card input.

If during enrollment, the User ID is taken from a card input, during authentication, you would need to present the same card. A user record that enrolled in this way is one that has an additional authentication factor, which is the card. In short, the card has to be presented before TouchStar can proceed to carry out the fingerprint verification.

Note:

If, during enrollment, the User ID was taken from a card input, the Speed Search and one-to-many search operations would fail on this record during authentication.

On the other hand, if during enrollment, the User ID is taken from the keypad input, during authentication, you can either present a card that has the same ID, or use the keypad to enter the ID. In addition, you can also enter 2 or more ending digits from the User ID to do a Speed Search. Lastly, you can also do the one-to-many matching.

b) Doing a card-only authentication:

If you enroll yourself as a card-only record, you simply need to scan your card across the device to authenticate.

c) Doing a card with PIN authentication:

If you enroll yourself using PIN, the User ID that is associated with this PIN can either come from the keypad input or a card input.

If during enrollment, the User ID is taken from a card input, during authentication, you would need to present the same card. Likewise, a record enrolled in this way as one that has an additional authentication factor, which is the card.

If during enrollment, the User ID is taken from the keypad input, during authentication, you can either present a card that has the same ID, or use the keypad to enter the ID.

Allowing the keypad input to replace the card input

You can override the requirement for the card to be present for fingerprint authentication or PIN authentication. To do so, please refer to “**Chapter 5.1.2l - Allowing Keypad Input to Replace Card Input for Fingerprint Verification (page 73)**” and “**Chapter 5.1.2m - Allowing Keypad Input to Replace Card Input for PIN Verification (page 74)**”.

Each user record can enroll more than one type of property

You can enroll each user record with more than one type of authentication properties. For example, you can enroll yourself with both fingerprint and PIN properties. This kind of enrollment, however, is only possible through the application program.

3.1.2 Understanding Speed Search and One-To-Many Search

Speed Search:

Speed Search is a fingerprint verification method distinctive in TouchStar. In Speed Search, you just need to enter 2 or more digits from the trailing part of your User ID to start a fingerprint verification.

For example, if your User ID is “5678”, you just need to enter “78” followed by the Green key. TouchStar would then ask you to place your finger. Your captured fingerprint would be then compared with all fingerprint records that ends with “78”. The comparison ends when a successful match is obtained.

Tips:

Speed Search is especially useful if your company uses a system where the User ID is significantly long and the employees have difficulty in remembering their own User IDs. With Speed Search, they can just enter 2 or more digits from the trailing part of their User IDs, instead of the entire length.

However, if there are many records that are similarly ending with the same 2 digits that you have entered, the search would take slightly more time. This is because all the fingerprint templates associated with the same last 2 digits have to be matched.

In order to speed up the search, you can enter more digits, such as 3 digits instead of the usual 2. By doing so, the number of records to search would be reduced.

One-To-Many Matching:

A term that is commonly used in biometrics, one-to-many matching or one-to-many search is also known as identification. The other common term is verification, which is also known as one-to-one matching.

In one-to-many matching, the User ID is not required to be presented. TouchStar would search through the complete fingerprint database to look for a match. In other words, you need not remember your User ID if you are doing a one-to-many matching.

However, one-to-many matching is operated on a higher security level as compared to normal verification. This is necessary in order to prevent false acceptances. In addition, searching time would increase with the number of fingerprints registered in the device.

Notes:

In identification, no User ID needs to be presented. The system searches through the complete fingerprint database until it is able to find a match. In verification, a User ID is presented. The fingerprint template(s) associated with this user record are matched with the presented fingerprint.

3.1.3 Understanding Multiple Fingerprint Verification

In usual operation, TouchStar only matches one fingerprint to successfully pass a verification.

In multiple fingerprint verification, it must match 2 or 3 fingerprints before considering the verification to be successful. This feature makes use of the fact that TouchStar is able to enroll up to 6 different fingerprints for a User ID.

If you are planning to use this feature, and intend to match 2 fingerprints, you would need to ensure that all user records are enrolled with at least 2 fingerprints.

The 2 or more fingerprints that are enrolled for a record can come from the same person, or from 2 or more different persons. If the fingerprints come from different persons, these persons need to be physically present to match their respective fingers before the verification can be passed.

Notes:

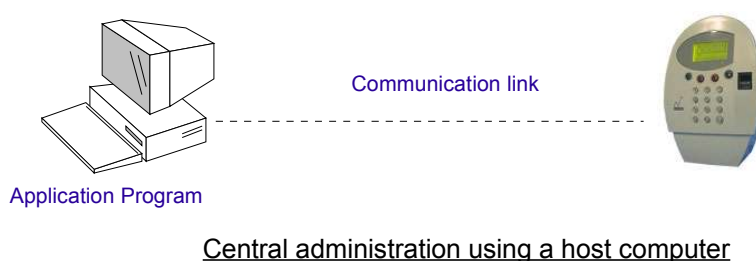
1. For users who are enrolled with less than the required number of fingerprints for multiple fingerprint verification, the matching will be rejected.
2. Speed Search and one-to-many search operations cannot be used when multiple fingerprint verification is enabled.

3.2 Central Administration

The TouchStar device comes with a central administration software (application program) that allows you to control the device, to enroll authentication properties and to download these properties to the devices.

The software comes in a few tiers. Each tier is packaged with different features to suit your needs. For example, you may not need all the features that are available in the highest tier. Please check with your dealer on the tier that suits your requirements.

For more details on central administration, please refer to the manual that comes with the software.



3.3 Timezone in TouchStar

There are 3 types of timezone control:

- **Personnel Schedule**
- **Door Schedule**
- **Bell Schedule**

Personnel Schedule

Personnel Schedule applies to users. It refers to TouchStar checking of a set of timings prior to carrying out the authentication for the users. For example, if you are doing a fingerprint authentication, TouchStar would check the timezone information assigned to you to ascertain that you are allowed access at the time of using the device.

When Personnel Schedule is active, users have to be grouped. Each group is associated with a schedule. A schedule corresponds to a set of periods (day and time), which the user can gain entry.

Door Schedule

Door Schedule applies to a door. It refers to the checking of a special schedule to automatically open or close the door. Please note that the Door Schedule only works with the TouchStar Door Zone Controller.

Bell Schedule

The last type of timezone control actually does not perform any access control. It uses the same timezone information such as the calendar to control the times at which an externally connected bell would ring for notification purposes.

Note:

1. Timezone information can only be defined through the application software:

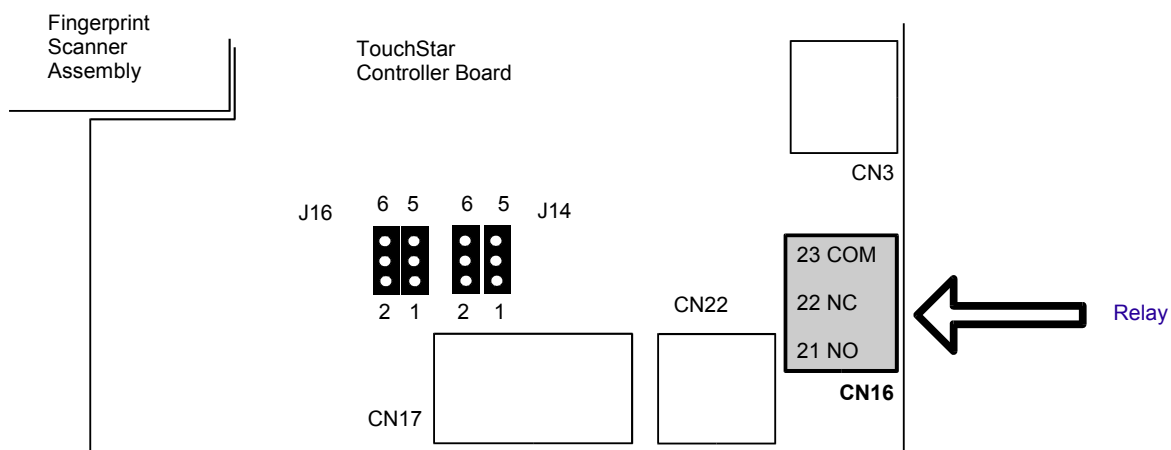
Timezone control can operate fully only when the timezone information has been downloaded to the device through the central administration software. The download information consists of the calendar, schedule and group information.

You can find out more information on timezone from the manual in the application program.

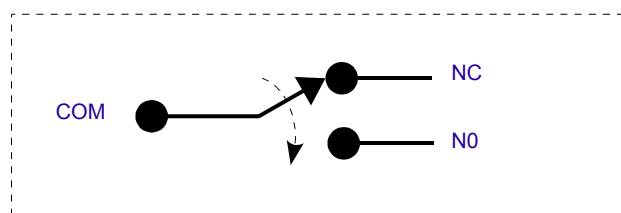
- 2.** The schedule number 88 is reserved for the Door Schedule, while the schedule number 99 is reserved for the Bell Schedule.

3.4 Using the Relay in TouchStar

TouchStar has an on-board relay (CN16) that can be used for a few purposes. It can be used to trigger a bell, trigger a turnstile, or light up a lamp upon a successful authentication. It can also be used to ring the bell at fixed times.



Location of relay in TouchStar controller board



How a relay works

How a relay works

A relay is an electromechanical 3-way switch. One end of the relay always rests at COM (common). The other end rests on either NC (normally closed) or NO (normally opened) at any time. It rests on NC when TouchStar is powered up and the relay is not triggered. When the relay is triggered, it switches to the NO position.

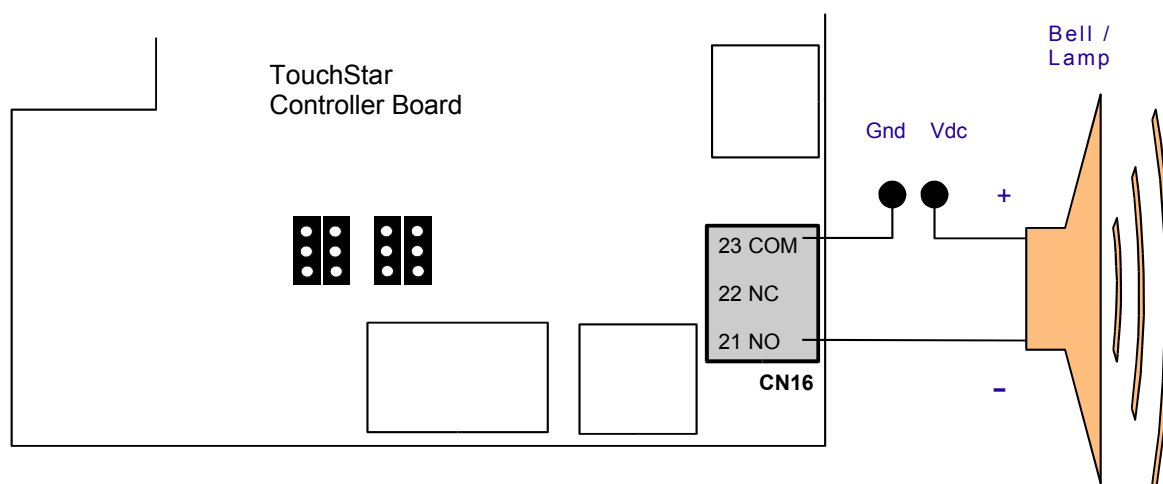
Using the relay to sound an externally connected bell or light upon a successful authentication

You can connect an external bell or lamp to the relay in TouchStar, and configure TouchStar to ring the bell or light up the lamp upon a successful authentication.

Using the relay to sound an externally connected bell at fixed times

You can also connect an external bell to the relay in TouchStar, and configure TouchStar to ring the bell at fixed times.

The times at which this bell shall ring can be configured in 2 ways. TouchStar can use a set of 20 bell timings that can be configured directly in the Master Page, or it can use a more flexible bell schedule that requires the central administration software. You can refer to more information on using the relay in **“Chapter 5.1.2e - Configuring the Relay Option (page 61)”**.



Connecting an external bell or lamp to the relay

Notes:

The use of the relay to directly control an electromagnetic lock for access control purposes is really not recommended. However, the schematics for doing so is still presented in “**Appendix D – Using the On-board Relay for Door Control (page 97)**”.

For a more secure installation, you may like to consider the use of the TouchStar Door Zone Controller, or any external door controller from a third party vendor.

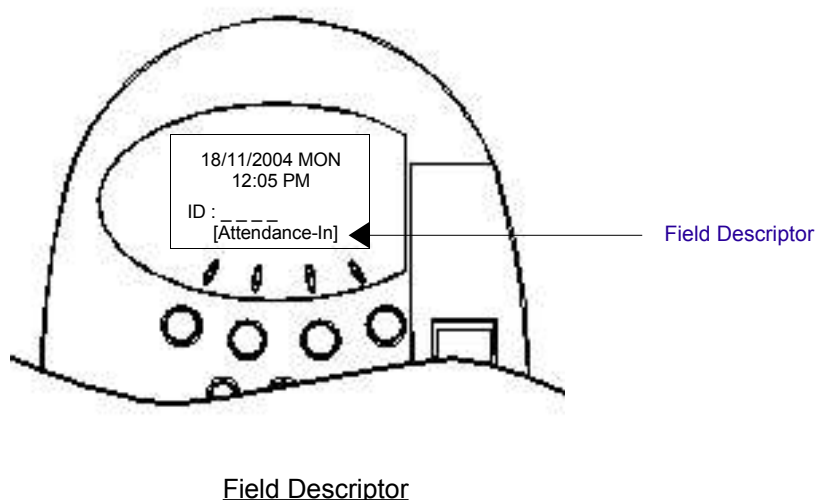
3.5 Logging

There are 4 types of log records in TouchStar.

a) Transaction (or Time Attendance)

A transaction log is recorded upon a successful authentication. Each log record contains the User ID of the user performing the authentication, the date and time, and the time attendance field descriptor (or log type).

There are a few sets of field descriptors that you can choose to use. One of these sets comprises the “In” and “Out” fields. When you are at the device, you need to select the field you want by pressing the Attendance Mode key. After the desired field has been displayed, you should then begin your authentication. Upon successful authentication, the transaction log would then carry this field descriptor.



The field descriptor is useful for knowing exactly when is the “in” transaction, and when is the “out” transaction.

b) Trace Event

A trace event log is recorded whenever any critical event occurs during local administration or during operation. An example of a trace event recorded during operation is when the tamper switch inside TouchStar was opened.

c) Fail Attempt

A fail attempt log is recorded when the authentication process fails. Each log would indicate the reason behind this failed attempt - whether the process fails because the User ID was not found, or a fingerprint matching operation had failed, or other reasons.

d) Authentication Mode Trace

An authentication mode trace log is recorded after the transaction log has been recorded. It records which authentication property was used to achieve the successful authentication. This log also indicates whether the ID was entered using the keypad, or was captured from a card scan.

Notes:

By default, only the transaction log is turned on.

The rest of the other logs are turned off. All these logs share the same log space. By turning off unnecessary logs, the log space would not fill up too quickly. TouchStar has a round-robin log space for 20,000 log records.

Tips:

When the full capacity is reached, the logs are over-written on a first-in-first-overwritten basis. Therefore, you need to ensure that log records are uploaded to the application program periodically to prevent loss of data.

3.5.1 Preventing Duplicated Log Records

Duplicated log records are those that have the same User ID, but a different time-stamp.

TouchStar has a feature to check for a duplicated log with the same User ID within a time frame. For example, if you had forgotten that you had previously clocked-in 5 minutes ago, and try to clock-in again, TouchStar would report a message that you had already clocked-in and prevent this current log from being recorded into the log space.

The time-frame to check for duplicated log records is user-configurable from 1 to 99 minutes.

3.5.2 Viewing Recent Log Records

Another feature of TouchStar is that it allows you to view your last 4 transaction logs from the User Page. This feature is useful in time-attendance applications where users may want to check their clocking-ins at the end of their working day.

3.6 Interfacing with Door Controllers through Wiegand

3.6.1 Third Party Door Controllers

TouchStar supports the following Wiegand formats to interface with external door controllers:

- 1) 26 Bits Standard
- 2) 26 Bits Vendor 1
- 3) 26 Bits Vendor 2
- 4) 32 Bits Standard
- 5) 34 Bits Standard
- 6) 35 Bits Standard
- 7) 36 Bits Standard
- 8) 37 Bits Standard
- 9) 40 Bits Standard

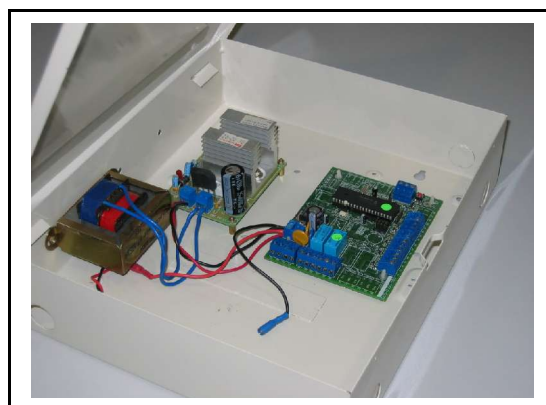
When the Wiegand output setting is enabled at the device, TouchStar would generate and send the Wiegand data (ID with site code and land code) to the external controller upon a successful authentication. For the Wiegand data to be recognizable, the external controller must also use the same Wiegand format.

3.6.2 TouchStar Door Zone Controller

TouchStar can also be configured to interface with the TouchStar Door Zone Controller. The picture on the left shows the controller board, while the one on the right shows how it looks like when mounted within an enclosure.



TouchStar Door Zone Controller Board



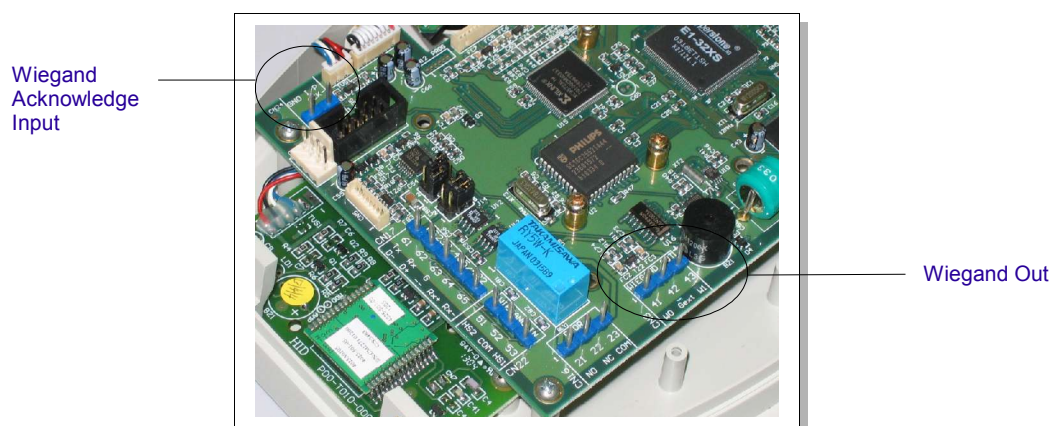
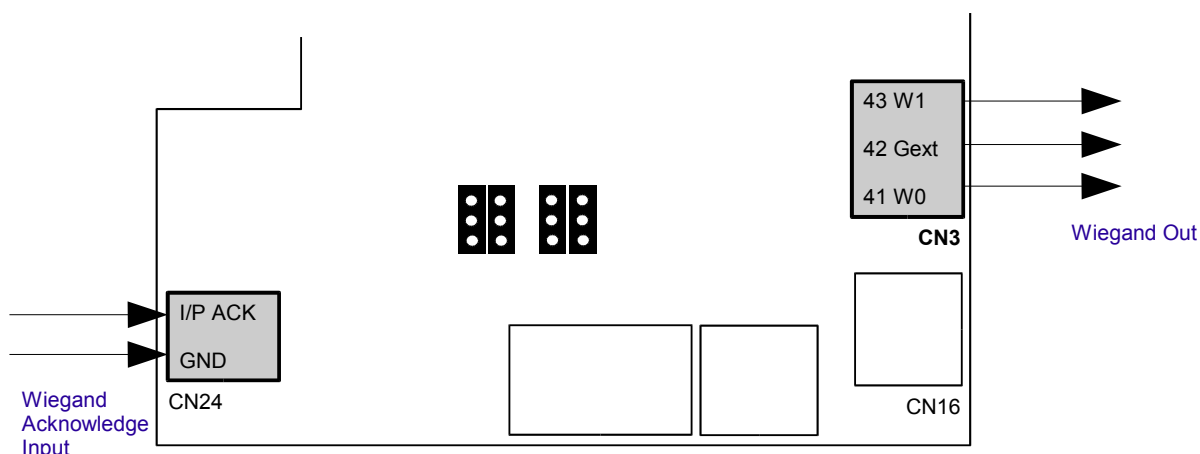
Controller Board mounted in enclosure

The TouchStar Door Zone Controller is a dedicated controller board, which provides two relay contact points. One of these points can be used to control the electro-magnetic lock. The other relay contact point can be used to trigger an alarm.

In addition, the door controller also provides door ajar and door exit sensing capability. You can refer to “**Appendix C – TouchStar Door Zone Controller (page 95)**” for a short description of this controller.

3.6.3 Waiting for an Acknowledgment Signal from External Controller to Indicate Receipt of Wiegand Sent

TouchStar can be configured to wait for an acknowledgement signal from the external controller to indicate that the Wiegand data it sent out previously upon a successful authentication had been properly received. In this operating mode, if TouchStar does not receive the acknowledgement signal, it would display a warning message at the User Page.



Location of Wiegand Out and Wiegand Acknowledge Input

3.6.4 Sending Special Wiegand Code to Indicate Failed Verification

TouchStar is able to send out reserved Wiegand codes upon a failed authentication. However, the receiving controller needs to understand the codes properly. The following codes are sent:

- 0001 – User ID is valid but fingerprint authentication failed.
- 0002 – User ID does not exist.

Chapter 4

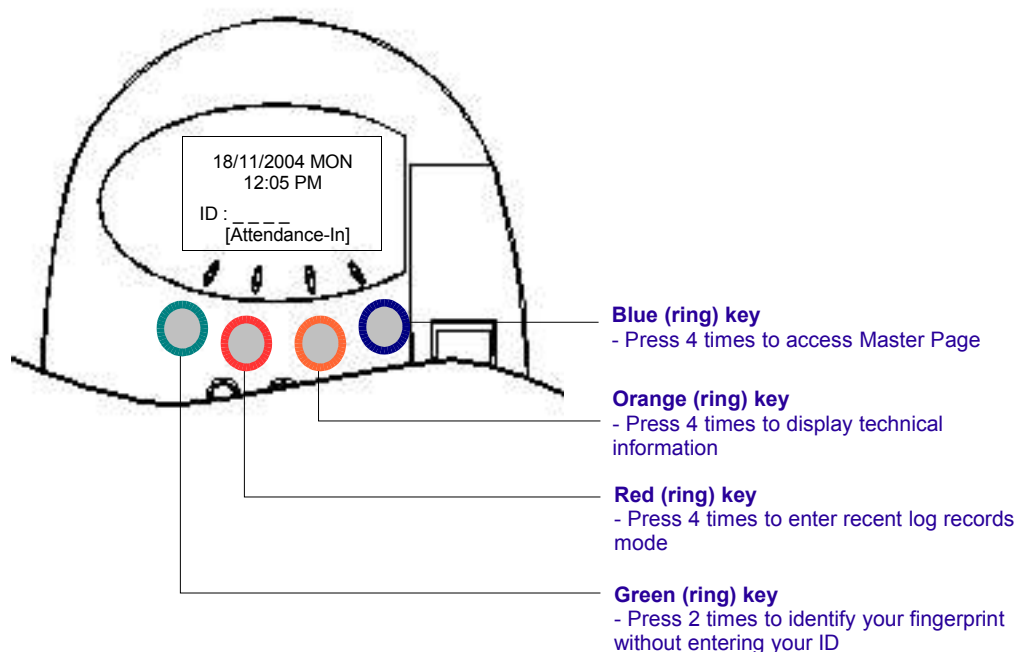
4 Basic Administration

The menu in TouchStar is easy to understand, navigate and use. There are 2 types of menus: the menus in the User Page and the menus in the Master Page.

4.1 Understanding and Using the User Page

The User Page is where you perform verification. In addition, you are also able to view the firmware version of TouchStar as well as other helpful information that would otherwise require you to enter the Master Page to find out.

For time attendance applications, the User Page also allows the users to view their last 4 transactions. The layout of the User Page and the purpose of the function keys are illustrated in the diagram below.



Purpose of the 4 function keys in the User Page

4.1.1 Performing Matching at the User Page

This section describes how matching (or authentication) can be carried out.

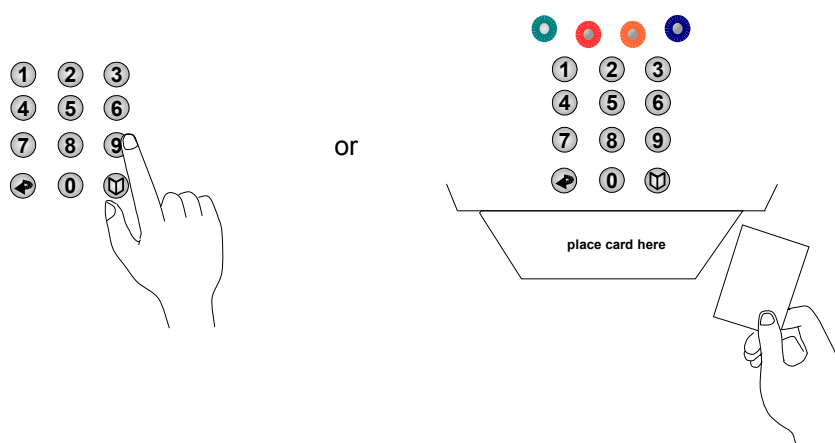
a. Fingerprint Matching

TouchStar can match a fingerprint in 3 ways. Upon a successful match, the screen would display “FP Accepted”.

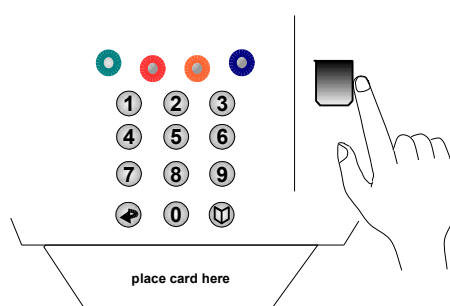
a) Verification (one-to-one matching)

- 1) Enter your User ID on the keypad or present your contactless card.

Note that if you enter your User ID, the user record associated with this User ID must be one that was originally enrolled without using the card to provide the ID. Otherwise, the device would reject and abort the matching. This is because the card is treated as an additional authentication factor.

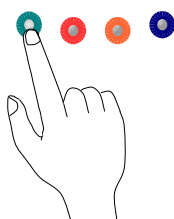


- 2) If the ID exists, the fingerprint sensor will light up to ask you to place your finger.



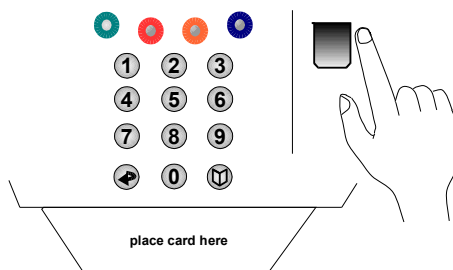
b) Identification (one-to-many matching)

- 1) Press the Green key twice.



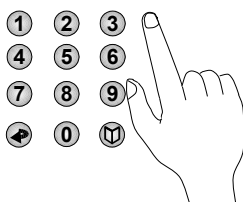
- 2) The fingerprint sensor would then light up to ask you to place your finger. Please refer to **“Chapter 5.1.1a - Setting the Security Level and Identify Mode (page 53)”** to ensure that this feature has been enabled.

Note that identification would fail on user records that are originally enrolled with the card being used to provide the ID. This is because the card is treated as an additional authentication factor.

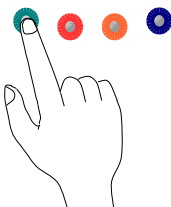


c) Speed Search

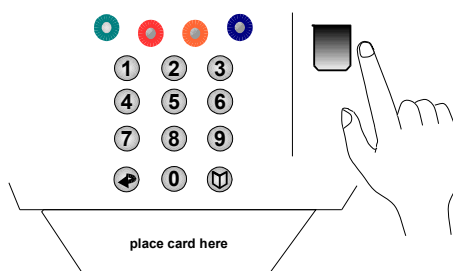
- 1) Enter 2 or more of your trailing User ID digits. For example, if your User ID is “1234”, enter “34”.



- 2) Press the Green key once.



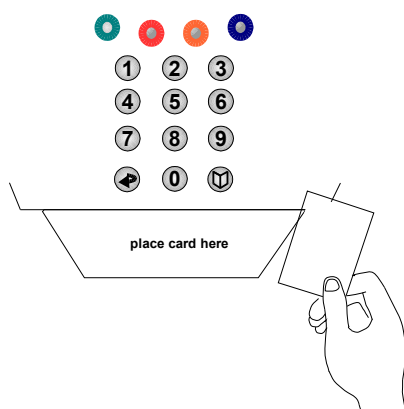
- 3) The fingerprint sensor would light up to ask you to place your finger.



Note that Speed Search would also fail on user records that are originally enrolled with the card being used to provide the ID. This is because the card is treated as an additional authentication factor.

b. Card Only Matching

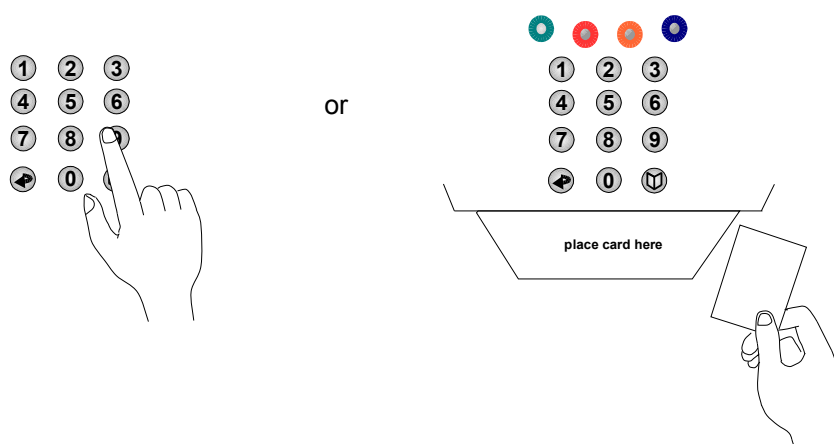
Present your card. Upon successful matched, the screen would display “Card Accepted”.



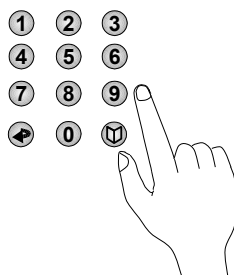
c. PIN Matching

- 1) Enter your User ID on the keypad or present your contactless card.

Note that if you enter your User ID, the user record associated with this User ID must be one that was originally enrolled without using the card to provide the ID. Otherwise, the device would reject and abort the matching. This is because the card is treated as an additional authentication factor.



- 2) If the User ID exists as a record enrolled with a PIN, the device would ask you to enter your PIN.



- 3) Upon successful matched, the screen would display “PIN Accepted”.

4.1.2 Viewing Recent Log Records

You can view your last 4 log transactions from the User Page. A typical use of this menu is for users who want to check whether they have clocked in properly for the day.

- 1) Press the Red key 4 times.



- 2) The following menu appears to ask you to enter your User ID.

Recent Log Rec	
Enter User ID	
ID: _____	
EXIT	

- 2) Enter your User ID number. If transaction log records belonging to the User ID exist, the last 4 transactions would be displayed. An example is shown below.

ID:1001		
	Date(DD/MM)	TIME
1.	15/06/2004	08:06
2.	15/06/2004	13:35
3.	16/06/2004	08:05
4.	16/06/2004	14:00
EXIT		

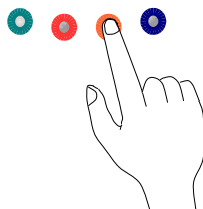
Note:

Only the transaction (or time attendance) logs are displayed. Other types of log events such as failed attempt logs, event trace logs and authentication mode trace logs are not.

4.1.3 Viewing TouchStar Technical Information

All configurations are done and viewed inside the Master Page. However, you can still view most of the basic ones from the User Page.

- 1) Press the Orange key 4 times.



- 2) You would see the following menu. The menu tells you the firmware version of the TouchStar device, its Device ID, version of the fingerprint unit and the serial number of the device. Other information is also available in another page.

Page 1

TouchStar Info.	
FIRMWARE	V8.005
RELEASE DATE	08/06/04
DEVICE ID	001
FP VERSION	V00.03
SERIAL NO.	A1000217
EXIT	PAGE
	E

- 3) Press the PAGE key to go to the other page. In this page, you can view the communication type, the operating baud rate, the Wiegand format and the fingerprint template capacity of the device.

Page 2

TouchStar Info.	
COMM TYPE	RS232
BAUD RATE	38400
WIEGAND	26 BITS-V1
LANGUAGE	ENGLISH
TEMPLATE	38400
EXIT	PAGE
	E

Tips:

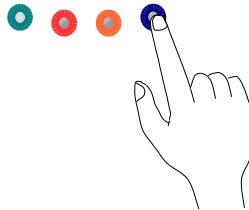
If you intend to send this unit back for warranty repairs, you would be asked for the serial number of the unit. This page allows you to know the serial number quickly.

4.2 Understanding and Using the Master Page

The Master Page is where configuration and enrollment are made. It is only accessible by a Master. Only a Master has the rights to enroll other users or to modify the settings. We would now look at how you can enter the Master Page.

4.2.1 Entering the Master Page

- 1) Press the Blue key 4 times.



If you are enrolling the first master of the device, you would be led to step 2.
If you have already enrolled the first master, you would be asked to place your finger for authentication. Go to step 3.

- 2) Enrolling the first master:

ADD MASTER=>FP			
Enter Master ID			
ID: _____			
■	EXIT	■	■

- i) Enter your User ID or scan your card across the card reader. When the full User ID has been entered, you would be asked to place your finger.

ADD MASTER=>FP1			
-> Place Finger			
ID: 1546			
■	EXIT	■	■

- ii) After the first capture has been obtained, you would be asked to lift your finger and place it on fingerprint sensor again to obtain the second capture.

ADD MASTER=>FP1			
-> Lift Finger			
ID: 1546			
	EXIT		

- iii) Enrollment is successful when you see the message, "FP Accepted". The menu in step 3 would be displayed.

- 3) Authenticating the master fingerprint:

AUTHENTICATION	
Verify Master FP	
-> Place Finger	

- i) Place your finger for the master authentication.
- ii) If the authentication passes, your User ID would be flashed across the page. The Master Page would be displayed next.

AUTHENTICATION	
Pass Authen.	
ID: 1546	



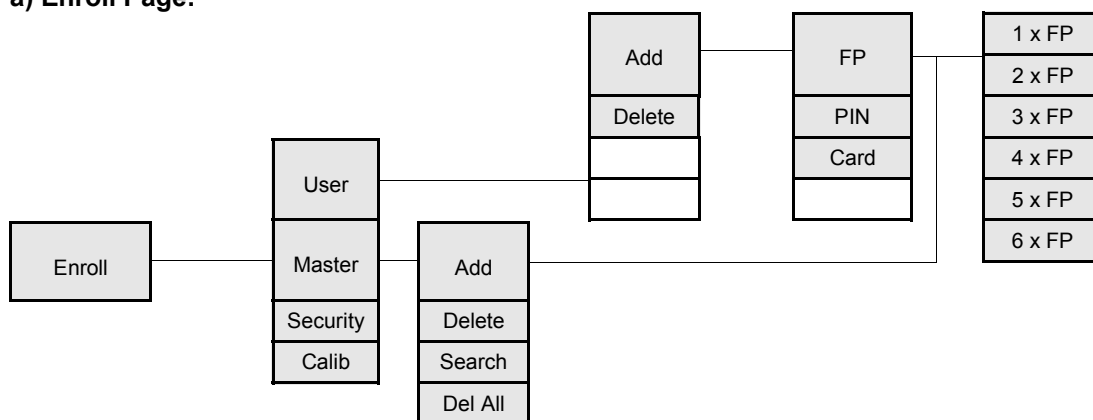
Master Page

ENROLLMENT			
User	Security		
Master	Calib		
SE I	EXIT	INFO	ENTER

4.2.2 Menu Map in the Master Page

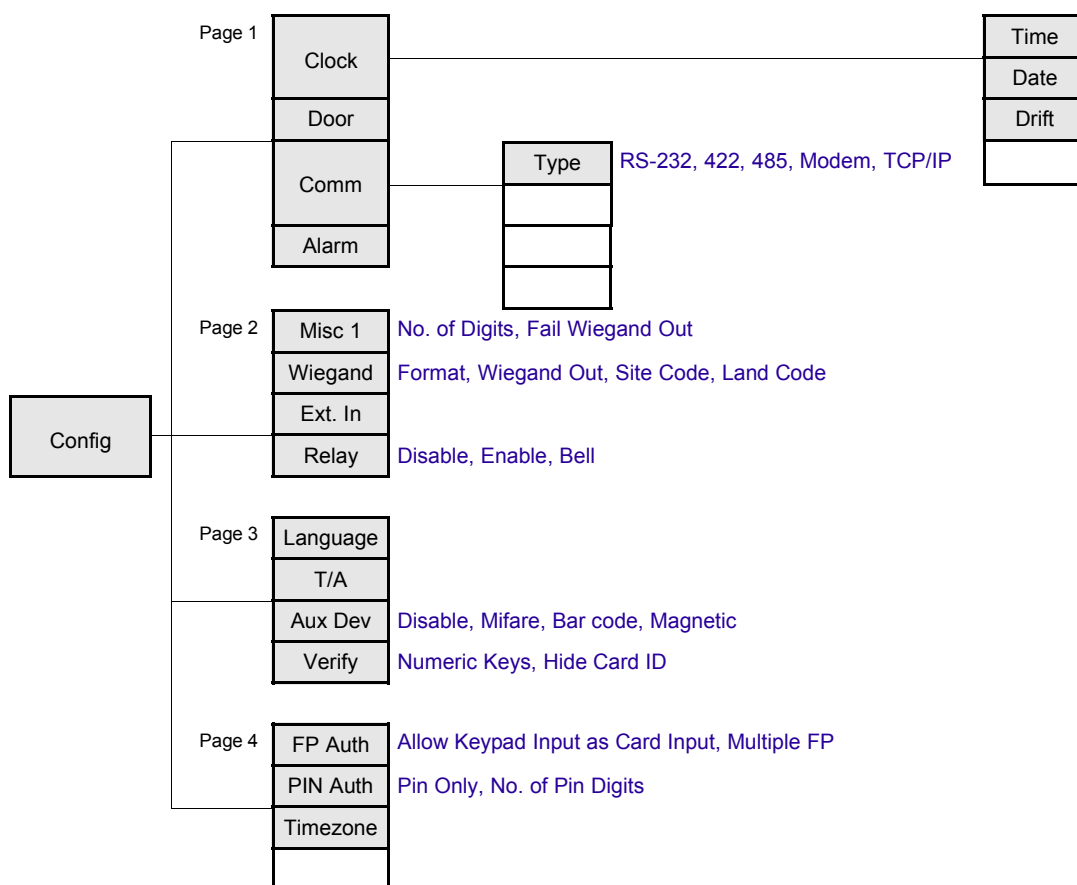
The Master Page has a hierarchical system. You can make use of the following chart to help you get to the setting you want in the Master Page.

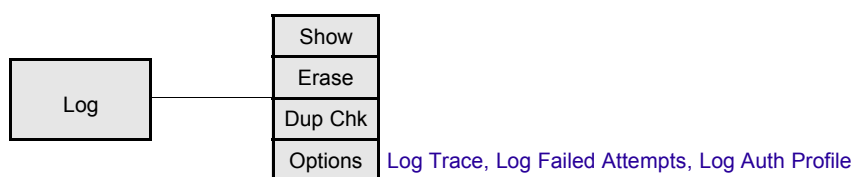
a) Enroll Page:



b) Config Page:

The Config page is split into 4 pages.



c) Log Page:**4.2.3 Navigating the Master Page (Read This)**

Navigating the Master Page is through the 4 function keys. Depending on where you are in the Master Page, the action associated with each function key is different.

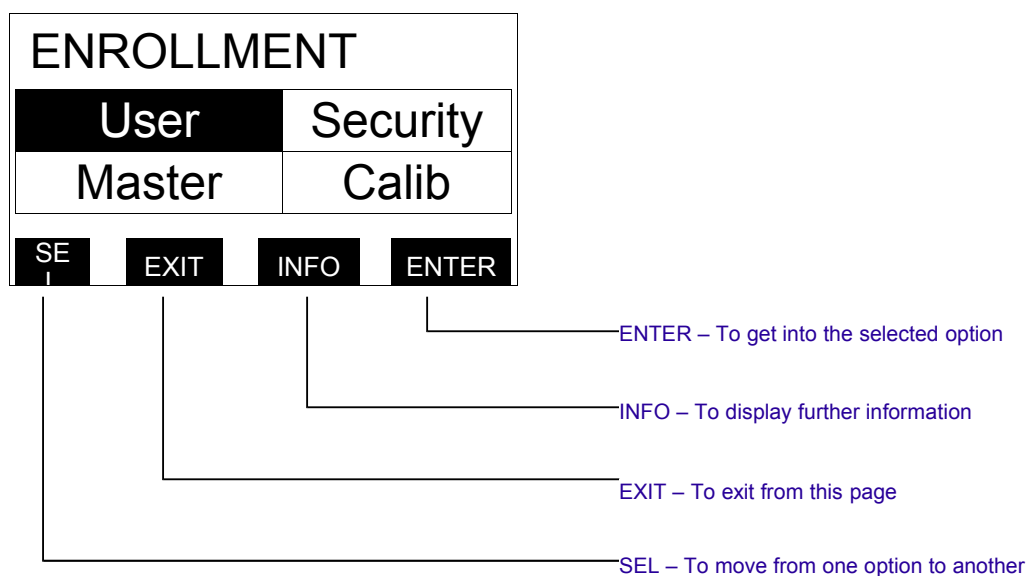
There are basically 2 types of menus in the Master Page.

a) A menu that would lead into another menu:

This menu is one where you can select the desired option and move on to another further menu. The usage of the 4 function keys are displayed at the bottom of the screen. Note that in some menus, no operation is associated with a particular function key. In others, an action is associated with it.

Example 1:

In this example, an INFO operation is associated with the third function key. Pressing this key allows you to view the number of users who are enrolled in the device.



Example 2:

In this example, a PAGE action is associated with the third function key. Pressing this key allows you to move from one page to another.

SYSTEM CONFIG			
Clock		Comm	
Door		Alarm	
SE I	EXIT	PAG E	ENTER

b) A menu that requires making settings:

In this type of menu, the action associated with each function key is different from that previously seen.

Example 3:

This example shows the common menu that you would see.

It comes with a field called "SETTING". The selection for "SETTING" can either be "[DEFAULT]" or "[CUSTOMIZE]".

"[DEFAULT]" means the settings within the menu are factory values. If you need to make modifications to the settings, you would need to change "[DEFAULT]" to "[CUSTOMIZE]" first before you can move on to the next rows.

Whenever you want to save the settings, press the EXIT key. The system would then prompt you to commit the saving.

SECURITY MODE			
SETTING : [DEFAULT]			
IDENTIFY : [ENABLE]			
SECURITY : 3			
SEL	EXIT		ENTER

ENTER – To move from one row to the next

No action in this menu

EXIT – To exit from this page. Upon pressing this key, the system would prompt you whether you would like to save the settings.

SEL – To change the current value. In this example, pressing the SEL key would change SETTING from DEFAULT to CUSTOMIZE

When the EXIT key is pressed ...



SECURITY MODE	
SETTING :	CUSTOMIZE
IDENTIFY :	DISABLE
SECURITY :	3
SAVE SETTING ?	
YES	NO

NO – To exit without saving the settings

YES – To save the settings and then exit

Example 4:

This example shows a menu that would be encountered in the CONFIG TCP/IP menu. Due to the many parameters that you would need to set, FWD and BACK keys are designed to allow you to move easily from one selected item to another.

CONFIG TCP/IP	
IP :	090.000.000.060
GW :	001.002.003.004
SUBNET MASK :	08
TCP/IP PORT :	03001
SEL	EXIT
BACK	FWD

FWD – To move forward from one selected item to the next

BACK – To move backwards from one selected item to the previous

EXIT – To exit from this page. Upon pressing this key, the system would prompt you whether you would like to save the settings.

SEL – To change the current value. In this example, pressing the SEL key would change 0 to 1

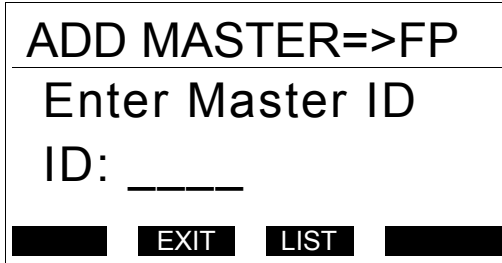
Summary for this Section

We have seen how you are able to navigate between the menus and how to save the settings within each menu. In the next few sections, we would look at the various menus in TouchStar.

4.2.4 Inside the ENROLL Page

a. Adding a Master

- 1) Go to ENROLL → Master → Add.



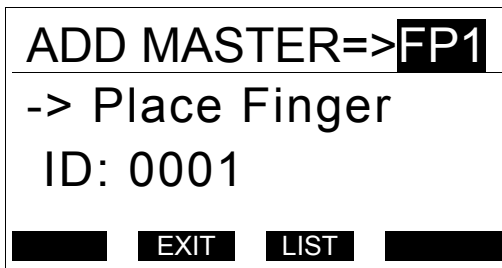
ADD MASTER=>FP

Enter Master ID

ID: _____

EXIT LIST

- 2) Enter your User ID or scan your card across the card reader. When the full User ID number has been entered, you would be asked to place your finger.



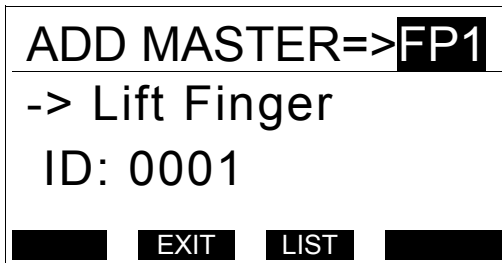
ADD MASTER=>FP1

-> Place Finger

ID: 0001

EXIT LIST

- 3) After the first capture has been obtained, you would be asked to lift your finger and place it on fingerprint sensor again to obtain the second capture.



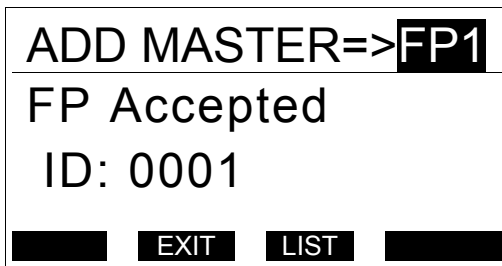
ADD MASTER=>FP1

-> Lift Finger

ID: 0001

EXIT LIST

Enrollment is successful if you see the message, "FP Accepted".



ADD MASTER=>FP1

FP Accepted

ID: 0001

EXIT LIST

Tips:

You can list the User ID of the masters already enrolled in TouchStar by pressing the LIST key.

b. Adding a User

Adding a User with Fingerprint:

- 1) Go to ENROLL → User → Add → FP. Select how many fingerprints you want to enroll. To enroll more than 4 fingerprints, use the PAGE key to change the page.

Page 1

USE HOW MANY FP?	
1 x FP	3 x FP
2 x FP	4 x FP

Page 2

USE HOW MANY FP?	
5 x FP	
6 x FP	

- 2) Enter your User ID or scan your card across the card reader.

ADD USER=>FP			
Enter User ID			
ID: 402_			
	EXIT		

- 4) When the full User ID number has been entered, you would be asked to place your finger.

ADD USER=>FP1			
-> Place Finger			
ID: 4026			
	EXIT		

After the first capture has been obtained, you would be asked to lift your finger and place it on fingerprint sensor again to obtain the second capture. Enrollment is successful if you see the message, "FP Accepted".

- 5) If you have selected 2 x FP, 3 x FP, 4 x FP, 5 x FP or 6 x FP, you would be prompted to place the next fingers for the next enrollment. Repeat from step 4 again.

ADD USER=>FP2			
-> Place Finger			
ID: 4026			
	EXIT		

Tips:

If you already had a User ID enrolled with 1 fingerprint in the past, and you would like to enroll a second fingerprint now, you can select 2 x FP directly. TouchStar would directly enroll you with the second fingerprint.

Adding a User with Card Only:

- 1) Go to ENROLL → User → Add → Card.

ADD USER=>CARD			
-> Present Card			
ID: _____			
	EXIT		

- 2) Scan your card across the card reader. Enrollment is successful if you see the message, “Add User Passed”.

ADD USER=>CARD			
Add User Passed			
ID: 5595			
	EXIT		

Adding a User with PIN:

- 1) Go to ENROLL → User → Add → PIN.

ADD USER=>PIN			
-> Present Card			
ID: _____			
■	EXIT	■	■

- 2) Scan your card across the card reader, or enter your User ID. The User ID would be displayed for a short while.

ADD USER=>PIN			
-> Present Card			
ID: 5597			
■	EXIT	■	■

- 3) Enter your PIN.

ADD USER=>PIN			
-> Register PIN			
PIN - ** _____			
■	EXIT	■	■

- 4) Enter the same PIN again for verification. Enrollment is successful if you see the message, “Add User Passed.”

ADD USER=>PIN			
-> Register PIN			
Verify - _____			
■	EXIT	■	■

Note:

If you enrolled the PIN record by scanning a card, you would need to use the card for subsequent authentication. If you enrolled the PIN record by entering the ID using the keypad, you can authenticate by scanning a card with the same ID, or enter the ID using the keypad, after which TouchStar would ask you to key in your PIN.

Tips:

The number of PIN digits is configurable from 4 to 6.





c. Deleting a Master

In this menu, you can delete a master as well as a user.

- 1) Go to ENROLL → Master → Delete.

DELETE MASTER			
Enter Master ID			
ID:	_____		
			

- 2) Scan your card across the card reader, or enter the User ID of the record to delete. If the User ID belongs to a master, you will see the message, “1 Master Deleted”. If the User ID belongs to a user, you would see the message, “1 User Deleted”.

DELETE MASTER			
1 Master Deleted			
ID:	0001		
			





d. Deleting a User

This menu only allows you to delete a user.

- 1) Go to ENROLL → User → Delete.

DELETE USER			
Enter User ID			
ID:	_____		
	 EXIT		

- 2) Scan your card across the card reader, or enter the User ID of the record to delete. You would see the message, “1 User Deleted”.

DELETE USER			
1 User Deleted			
ID: 4001			
	 EXIT		

e. Searching for a Master Or User

- 1) Go to ENROLL → Master → Search. You would be asked to place your finger. TouchStar would then search for the User ID that corresponds to your fingerprint.

SEARCH	
-> Place Finger	

- 2) If the fingerprint matches with a device user in the device, you would see the message, “User Found”. If it matches with a device master, “Master Found” would be shown.

SEARCH	
User Found	
ID: 4001	

f. Deleting all User Records from Device

This operation would delete all user records (inclusive of masters) from the device. To protect this operation from accidentally being carried out, a master authentication is required.

- 1) Go to ENROLL → Master → Del All.

DELETE ALL USER

Are you sure ?

YES **NO**

- 2) Press YES to proceed with the operation. You would be asked to place your finger for the master authentication.

AUTHENTICATION

Verify Master FP
-> Place Finger

- 3) Press YES to proceed with the operation. You would be asked to place your finger for the master authentication. If the authentication passes, the deletion would start. The process would take about 30 seconds.

DELETE ALL USER

Deleting All FP
Please Wait ...

4.2.5 Inside the CONFIG Page

The menus inside the CONFIG page are quite similar to one another. Please refer to “**Chapter 4.2.3 - Navigating the Master Page (page 29)**” to learn how to navigate. In this way, the rest of the description here would be easily understood.

a. Setting the Time

How to get to menu:

Go to CONFIG → Clock (1st page) → Time.

SET TIME			
12 HOUR MODE HH:MM:SS			
11:10:58 AM			
SEL	EXI T		ENTER

12 Hour Mode

How to change the settings:

- 1) To change the time display from 12 hour mode to 24 hour mode, press the SEL key when the selection (cursor) is on the first line.

SET TIME			
24 HOUR MODE HH:MM:SS			
11:10:58 HR			
SEL	EXI T		ENTER

24 Hour Mode

- 2) Move the selection using the ENTER key. Use the SEL key to toggle the selected digit. Repeat this step for the rest of the digits until the desired time is set.

SET TIME			
24 HOUR MODE HH:MM:SS			
11:15:58 HR			
SEL	EXI T		ENTER

Changing the minute

- 3) Press EXIT to save the settings.

b. Setting the Date

How to get to menu:

Go to CONFIG → Clock (1st page) → Date.

SET DATE			
DD/MM/CCYY FORMAT			
10/11/2004 WED			
SEL	EXI T		ENTER

DD/MM/CCYY Format

How to change the settings:

- 1) To change the date display from the DD/MM/CCYY to the MM/DD/CCYY format, press the SEL key when the selection is on the first line.

SET DATE			
MM/DD/CCYY FORMAT			
11/10/2004 WED			
SEL	EXI T		ENTER

MM/DDCCYY Format

- 2) Move the selection using the ENTER key. Use the SEL key to toggle the selected digit. Repeat this step for the rest of the digits until the desired date is set.

SET DATE			
MM/DD/CCYY FORMAT			
11/11/2004 THU			
SEL	EXI T		ENTER

- 3) Press EXIT to save the settings.

c. Setting the Door Control

If you are using TouchStar for access control, you can either make use of the Wiegand output signal to inform the door controller to release the lock that it controls, or the on-board relay to directly control an external lock (not really recommended), or. For both situations, this menu needs to be set appropriately.

How to get to menu:

Go to CONFIG → Door (1st page).

CONFIG DOOR			
SETTING : [DEFAULT]			
LOCK DOOR : DISABLE			
SEL	EXIT		ENTER

Description:

	Setting	Purpose	Available Selections
1	LOCK DOOR	To control how should TouchStar control the door.	<p>a) DISABLE – Door is locked at normal times. When authentication passes, door opens. This is the normal selection.</p> <p>b) YES – Door is locked at all times. Even when authentication passes, door remains locked.</p> <p>c) NO – Door is never locked.</p> <p>d) SCHEDULE – Door automatically locks and unlocks by following a Door Schedule.</p> <p>If this selection is chosen, the calendar and door schedule must be present within the device.</p> <p>Please see “Chapter 3.3 - Timezone in TouchStar (page 13)”.</p>

How to change the settings:

- 1) To change the LOCK DOOR setting to other selections, use the SEL key to change SETTING from [DEFAULT] to [CUSTOMIZE].
- 2) Use the ENTER key to move the cursor to the second line, so that the LOCK DOOR selection can be changed.
- 3) After changing, press EXIT to save the settings.

Remarks:**a) Using the on-board relay to control the door:**

If you are making use of the on-board relay to directly control the door, you also need to configure the relay settings correctly. To understand how to set the relay, please go to CONFIG → Relay. Please see “**Chapter 5.1.2e - Configuring the Relay Option (page 61)**”.

b) Using Wiegand output signal to control the door:

If you are making use of the Wiegand output, besides making the correct settings here, you also need to choose the correct Wiegand format and make the correct Wiegand settings. To understand how to make the Wiegand settings, please go to CONFIG → Wiegand (see “**Chapter 4.2.5f - Configuring the Wiegand Settings (page 48)**”).

Notes:

The use of the relay to directly control an electromagnetic lock is not recommended. For a more secure installation, the use of the TouchStar Door Zone Controller, or any external door controller from a third party vendor is advised.

d. Setting the Communication Type as RS-232, RS-422, RS-485, Modem or TCP/IP

The communication type is a setting that enables the device to handle proper handshaking.

How to get to menu:

Go to CONFIG → Comm (1st page) → Type.

SET COMM TYPE

SELECT → RS232

SEL
EXIT

ENTE
R

Description:

	Setting	Purpose	Available Selections
1	COMM TYPE	To set the communication type.	a) RS232 b) RS422 c) RS485 d) MODEM e) TCP/IP

How to change the settings:

- 1) Use the SEL key to choose the COMM TYPE you want.
- 2) Press the ENTER key next to get into the menu for the selected type. The various menus are shown under the **Remarks** section below.

Remarks:**a) Menus for RS-232, RS-422 and RS-485:**

The menus for RS-232, RS-422 and RS-485 are similar. Each comprises the BAUD RATE and COMM ID settings.

```

CONFIG RS232
SETTING : [DEFAULT]
BAUD RATE : 38400
COMM ID : 001

SEL  EXIT  ENTER
  
```

```

CONFIG RS422
SETTING : [DEFAULT]
BAUD RATE : 38400
COMM ID : 001

SEL  EXIT  ENTER
  
```

```

CONFIG RS485
SETTING : [DEFAULT]
BAUD RATE : 38400
COMM ID : 001

SEL  EXIT  ENTER
  
```

Menus for RS-232, RS-422 and RS-485

	Setting	Purpose	Available Selections
1	BAUD RATE	To set the baud rate (bps). The baud rate chosen must be the same as that at the application program.	1200, 2400, 9600, 19200, 38400
2	COMM ID	To set the Device ID of the device.	1 to 254

b) Menu for MODEM:

TouchStar supports 2 types of modems, namely external and internal. Please consult your dealer if you wish to acquire the internal modem. The internal modem has a country code setting that has to be configured separately from the external modem.

As you select the COMM TYPE as MODEM, TouchStar would try to detect whether a modem (external or internal) is connected. If it fails to detect a modem, it would report an error message, "Modem was not found". However, if a modem is detected, TouchStar would ask you whether this is a external or internal modem.

```

SET MODEM TYPE

SELECT → EXTERNAL

SEL  EXIT  ENTER
  
```

Selecting type of modem – external or internal

Select the proper type of modem and press the ENTER key to get into its menu.

The menu for the external modem is similar to RS232, RS422 and RS485. For the internal modem, there is an extra setting for the country code as shown below:

CONFIG INT.MODEM	
SETTING :	DEFAULT
BAUD RATE :	38400
COMM ID :	001
COUNTRY :	U.S.A.
SEL	EXIT ENTER

Configuring the internal modem

Different telephone standards prevail in different countries. Selecting the correct country code is important for the internal modem to function correctly in your country. Please consult your local dealer on this.

c) Menu for TCP/IP:

If you have selected the COMM TYPE as TCP/IP and the Ethernet board (ECom) is present, you would see the following menu:

CONFIG TCP/IP	
IP :	090.000.000.060
GW :	001.002.003.004
SUBNET MASK :	08
TCP/IP PORT :	03001
SEL	EXIT BACK FWD

Menu for TCP/IP

The meaning of each parameters are explained as follows:

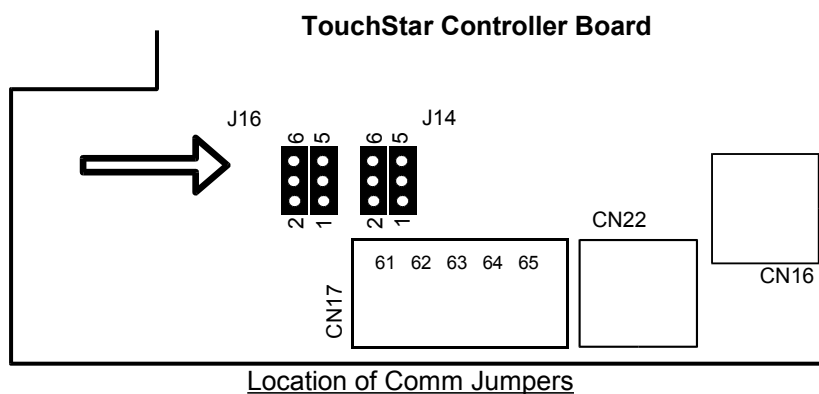
	Setting	Purpose	Available Selections
1	IP	To set the IP address.	Any valid IP address
2	GW	To set the gateway.	Any valid gateway address
3	SUBNET MASK	To set the subnet mask.	01 to 24 (The subnet mask setting here is translated to the actual subnet. The translation table is shown in the appendix.)
4	TCP/IP PORT	To set the TCP/IP port.	Any valid TCP/IP port.

d) Placement of Comm Jumpers:

For the communication channel to be established successfully, it is not sufficient to set the COMM TYPE correctly.

There is also a set of 4 jumpers (J14 to J16) that needs to be properly placed. These 4 jumpers controls the type of hardware signals that travels through the board and the interconnecting cables.

To understand how to place the jumpers, please refer to “**Chapter 6 - Setting Up for Communication (page 78)**”.

**e) Difference between RS-232, RS-422 and RS-485:**

When you select RS-232, TouchStar would reply to all commands send to it. This means that even if the command is not addressed to the unit, it would also reply with an error stating so.

On the other hand, if you select RS-422 or RS-485, TouchStar only replies to those commands that are addressed to the unit. If it receives a command that is not addressed to it, it would silently purge it. This means that the sender (application program) would not know if the unit it sent to has received it, or the transmitted command was lost in transit.

e. Setting the Alarm

The alarm in TouchStar is an indication that an event that violate normal operations has occurred.

Understanding more about this setting:

a) When is the alarm triggered?

The alarm mechanism in TouchStar is triggered during the following events:

(i) Tamper switch in TouchStar is opened:

If you opened up the TouchStar casing, you would be able to see the tamper switch. It is located at the top. When the casing is opened, the tamper switch is left open-circuited. This triggers the alarm.

(ii) Alarm mechanism in TouchStar Door Zone Controller was triggered:

If you are using TouchStar with the TouchStar Door Zone Controller, an alarm event that occurred at the door controller would be relayed back to TouchStar through the ACK line, which would subsequently trigger the alarm. Please see **Chapter 7.2 - Using the TouchStar Door Zone Controller (page 91)**.

The event that triggers the alarm at the controller can be the door sensing mechanism, its own tamper mechanism, or its evacuation mechanism.

b) How do you know if the alarm has been triggered?

When the alarm has been triggered, the only way to know is through the display indication at the LCD. A message, "Alarm Activate" appears on the display.

If the TouchStar Door Zone Controller is used, the controller would also be informed of such an event. The controller has a relay that you can connect to an external chime, siren or LED so that you are able to know by means of an audio or visual indication.

How to get to menu:

Go to CONFIG → Alarm (1st page).

CONFIG ALARM

SETTING
: DEFAULT

TYPE
: ENABLE

SEL
EXIT

ENTER

Description:

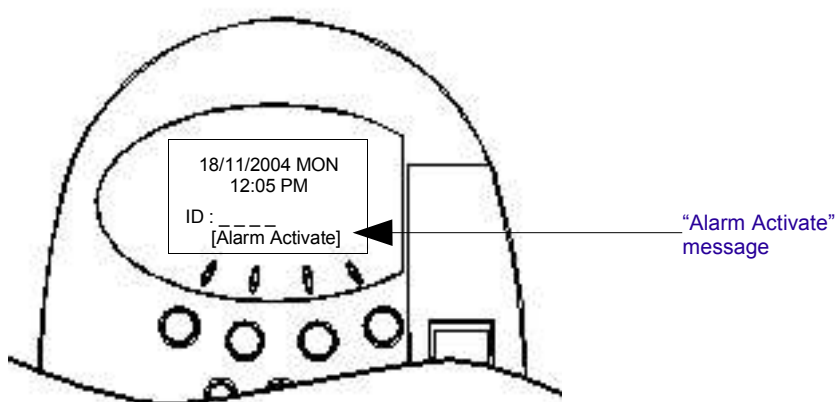
	Setting	Purpose	Available Selections
1	TYPE	To enable or disable the alarm. When the alarm is disabled, it would not be triggered even when the above events occurred.	ENABLE / DISABLE

How to change the settings:

- 1) If you wish to disable the alarm, use the SEL key to change SETTING from [DEFAULT] to [CUSTOMIZE].
- 2) Press the ENTER key to move the cursor to the next row.
- 3) Use the SEL key to change TYPE from ENABLE to DISABLE.
- 4) Press EXIT to save the settings.

Remarks:

When the alarm is enabled and has been triggered, “Alarm Activate” would be displayed on the screen as shown below:



Alarm Indication in TouchStar

f. Configuring the Wiegand Settings

The Wiegand settings allows you to configure a number of parameters.

Firstly, you can set the format. The format is necessary for knowing how to read a contactless card of Wiegand interface, as well as for knowing how to send out Wiegand codes to a controller upon a passed authentication.

Secondly, it allows you to enable or disable the sending of Wiegand codes upon a successful authentication.

Lastly, it allows you to set the site code and land code that would be used as part of the Wiegand signal if no site code or land code can be obtained from the user record for sending.

How to get to menu:

Go to CONFIG → Wiegand (2nd page).

CONFIG WIEGAND	
FORMAT :	26 BITS V1
WIEGAND OUT :	TS CONT
SEL	EXIT
	ENTER

Description:

	Setting	Purpose	Available Selections
1	FORMAT	To select the Wiegand format for reading the contactless card as well as for sending the ID code.	a) 26 BITS f) 35 BITS b) 26 BITS V1 g) 36 BITS c) 26 BITS V2 h) 37 BITS d) 32 BITS i) 40 BITS e) 34 BITS
2	WIEGAND OUT	For third party door controllers, to enable (set to ENABLE) or disable (set to DISABLE) the sending of Wiegand ID code upon a successful authentication. Or Whether to use the TouchStar Door Zone Controller (set to TS CONT).	a) TS CONT b) DISABLE c) ENABLE
3	SITE CODE	To set the site code that would be used as part of the Wiegand out signal if the Wiegand format chosen has a site code field. This site code is used if no site code can be obtained from the user record for sending.	The range depends on the Wiegand format chosen. In addition, some formats do not have a site code field at all. See Remarks .
4	LAND CODE	To set the land code that would be used as part of the Wiegand out signal if the Wiegand format chosen has a land code field. This land code is used if no land code can be obtained from the user record for sending.	The range depends on the Wiegand format chosen. In addition, some formats do not have a land code field at all. See Remarks .

How to change the settings:

- 1) Use the SEL key to change the FORMAT.
- 2) Press the ENTER key to move the cursor to the next row (WIEGAND OUT).
- 3) Use the SEL key to change the WIEGAND OUT setting.
- 4) If WIEGAND OUT is set to ENABLE, depending on the chosen format, the SITE CODE and LAND CODE fields would be displayed, allowing you to change these fields as well.
- 5) If the chosen format has a site code field and a land code field, press the ENTER key to move the cursor to these rows.
- 6) Use the SEL key to toggle the digits for the SITE CODE and LAND CODE fields.
- 7) Use the ENTER key to move from one digit to another.
- 8) When all the settings are completed, press EXIT to save the settings.

Remarks:**a) Choosing WIEGAND OUT as TS CONT:**

When this selection is chosen, there is no need to set the SITE CODE and LAND CODE fields.

b) How to choose the correct Wiegand format:

The Wiegand formats commonly used are 26 Bits Standard and 26 Bits V1. If you are not sure which Wiegand format to use, do check with the supplier of your contactless cards the format that the cards are programmed with.

Next, do try these cards on TouchStar to ensure the Card IDs are being read and displayed correctly.

c) Wiegand formats' specifications:

The following table illustrates some basic specifications of the various Wiegand formats. Use this table to help you choose the format if you are not sure which one to use.

	Format	Card ID Range	Site Code Range	Land Code Range
1	26 Bits	1 to 65535	0 to 255	x
2	26 Bits V1	1 to 65535	0 to 255	x
3	26 Bits V2	1 to 16777215	x	x
4	32 Bits	0 to 4294967295	x	x
5	34 Bits	0 to 4294967295	x	x
6	35 Bits	1 to 1048575	0 to 4095	x
7	36 Bits	1 to 16383	0 to 4095	0 to 255
8	37 Bits	1 to 1048575	0 to 1023	0 to 7
9	40 Bits	0 to 4294967295	x	x

x – The selected Wiegand format does not have this field.

g. Enabling or Disabling Timezone Checking

The checking of timezone here applies to the **Personnel Schedule** (see “**Chapter 3.3 - Timezone in TouchStar (page 13)**”).

This setting is disabled by default. Before you enable the setting, do ensure that all the necessary timezone information have been downloaded from the application program.

How to get to menu:

Go to CONFIG → TimeZone (4th page).

CONFIG TIMEZONE	
SETTING :	[DEFAULT]
TIMEZONE :	DISABLE
SEL	EXIT
	ENTER

Description:

	Setting	Purpose	Available Selections
1	TIMEZONE	To enable or disable the checking of timezone (Personnel Schedule)	ENABLE / DISABLE

How to change the settings:

- 1) To set TIMEZONE to ENABLE, use the SEL key to change SETTING from [DEFAULT] to [CUSTOMIZE].
- 2) Press the ENTER key to move the cursor to the next row.
- 3) Use the SEL key to toggle the TIMEZONE setting from DISABLE to ENABLE.
- 4) Press EXIT to save the settings.

4.2.6 Inside the LOG Page

a. Display all the Logs

How to get to menu:

Go to LOG → Show.

LOG					PG:1/2
0001	001234	0800	1211	01	
0002	001567	0801	1211	01	
0003	001433	0801	1211	01	
0004	001565	0802	1211	01	
0005	002100	0803	1211	01	
TOP	NEX	PRE	END		

Log Type (=1)

Date (=12 Nov)

Time (=0803 hrs)

User ID (=2100)

Running index (=5)

How to change the settings:

You can look at more log records by using the 4 function keys. The purpose of each key is described below:

TOP	- To go to the first page.
NEXT	- To go to the next page.
PREV	- To go back to the previous page.
END	- To go to the last page.

Press any other numeric key - To return to the previous menu.

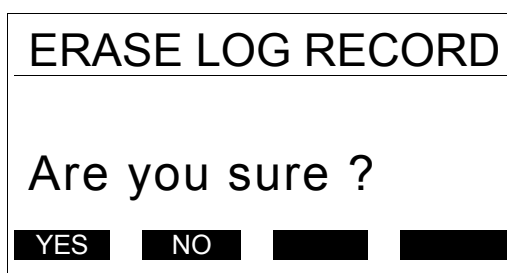
b. Erasing all the Logs

Log records are stored in TouchStar in a circular manner. The first block of log records that are written would be overwritten to make way for new log records when the capacity is reached.

You can choose to erase all log records if you need to. To ensure that you are performing the correct function, TouchStar would require a master fingerprint verification.

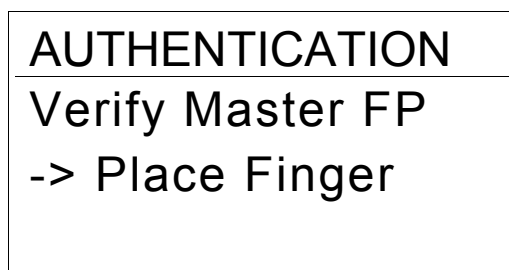
How to get to menu:

Go to LOG → Erase.

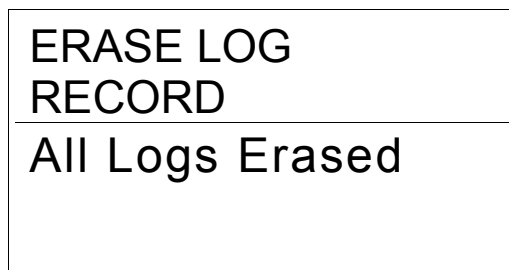


How to change the settings:

- 1) Press YES to go ahead with the erase operation.
- 2) TouchStar requires the master fingerprint verification. It would prompt you to place a master finger for the verification.



- 3) After the verification is successful, the erase operation would take place.
- 4) After the erase operation is completed, TouchStar would report a message:



The erase operation is now completed.

Chapter 5

5 Advanced Administration

This chapter describes more advanced usage of TouchStar. As in the last chapter, the description is categorized according to the menu layout.

5.1 In the Master Page

5.1.1 In the ENROLL Page

Please refer to “**Chapter 4.2.3 - Navigating the Master Page (page 29)**” to learn how to navigate. In this way, the rest of the description here would be easily understood.

a. Setting the Security Level and Identify Mode

The Security Level setting controls the level that fingerprint matching is carried out. This only applies to The higher the level, the more stringent is the matching being performed. On the other hand, the Identify Mode setting controls whether one-to-many search is enabled.

How to get to menu:

Go to ENROLL → Security.

SECURITY MODE	
SETTING :	DEFAULT
IDENTIFY :	ENABLE
SECURITY :	3
MASTER CARD/PIN :	NO
SEL	EXIT
	ENTER

Description:

	Setting	Purpose	Available Selections
1	IDENTIFY	To enable or disable the one-to-many search.	ENABLE / DISABLE
2	SECURITY	To change the security level used in Speed Search and one-to-one fingerprint verification. The higher the security level, the more stringent is the verification.	3 to 9

How to change the settings:

- 1) To change the Security Level or Identify Mode, use the SEL key to change SETTING from [DEFAULT] to [CUSTOMIZE] first.
- 2) Press the ENTER key to move the cursor to next row.
- 3) Use the SEL key to toggle the IDENTIFY setting from ENABLE to DISABLE (to disable the Identify Mode).
- 4) Press the ENTER key to move the cursor again to the next row.
- 5) Use the SEL key to change the SECURITY setting.
- 6) Press EXIT to save the settings.

b. Allowing Device Masters to Be Enrolled as Card Only or PIN

If you notice, when you press 4 times of the Blue key, the device authenticates you by using fingerprint matching.

Actually, the device is also able to authenticate you using Card Only or PIN when you enter the Master Page. However, this feature is disabled by default. As a result, you are only able to enroll or authenticate masters using fingerprint. To enable this feature, the MASTER CARD/PIN setting needs to be configured appropriately.

How to get to menu:

Go to ENROLL → Security.

SECURITY MODE			
SETTING	:	[CUSTOMIZE]	
IDENTIFY	:	[ENABLE]	
SECURITY	:	3	
MASTER CARD/PIN	:	YES	
SEL	EXIT	BACK	ENTER

Description:

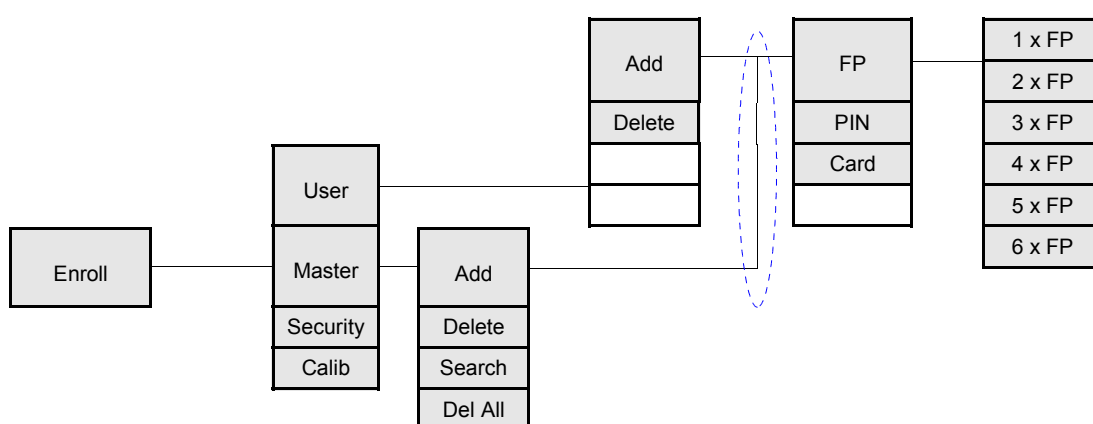
	Setting	Purpose	Available Selections
1	MASTER CARD/PIN	To allow device masters to be enrolled as a Card Only or PIN record.	Yes / No

How to change the settings:

- 1) If the SETTING is at [DEFAULT], use the SEL key to change SETTING from [DEFAULT] to [CUSTOMIZE].
- 2) Press the ENTER key to move the cursor to MASTER CARD/PIN row.
- 3) Use the SEL key to change the MASTER CARD/PIN setting from NO to YES.
- 4) Press EXIT to save the settings.

Remarks:**a) Change of menu map when MASTER CARD/PIN is set to YES**

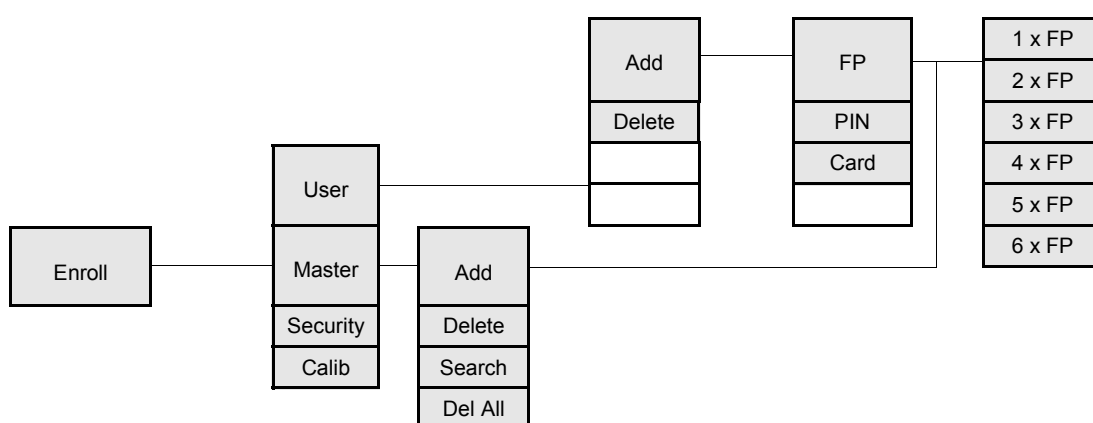
When the feature is enabled, the menu map for **Enroll** would be changed to the following:



New menu map for Enroll when MASTER CARD/PIN is set to YES

As you can see, besides fingerprint, a master can now be enrolled with Card Only and PIN.





The old menu map is shown below for comparison:



Menu map for Enroll when MASTER CARD/PIN is set to NO

b) Master authentication procedure is also changed when MASTER CARD/PIN is set to YES

When this feature is enabled, the master authentication procedure is changed slightly. When you press 4 times of the Blue key, instead of asking you to place your finger immediately, the following menu is shown:

AUTHENTICATION			
Enter Master ID			
ID:	_____		
			

Press the FP key to start fingerprint authentication immediately.

Otherwise, if you intend to authenticate the master who has been enrolled as Card Only or PIN, scan the card across the card reader.



If the master has been enrolled as Card Only, the authentication passes immediately. If it has been enrolled as PIN, the device would prompt you to enter the PIN.

c. Viewing the Fingerprint Sensor's Calibration Settings

This page is only for informative purposes. It allows you to check the calibration parameters for the fingerprint sensor. TouchStar does not allow you to change the settings.

How to get to menu:

Go to ENROLL → Calib.

CALIBRATION	
CURRENT VALUES -	
GAIN	: 40
CONTRAST	: 0
BRIGHTNESS	: 200
	

Description:

	Setting	Purpose	Available Selections
1	GAIN	Gain value of the sensor	For reading only
2	CONTRAST	Contrast value of the sensor	For reading only
3	BRIGHTNESS	Brightness value of the sensor	For reading only

5.1.2 Inside the CONFIG Page

a. Setting the Clock Drift Adjustment

This setting is meant for compensating the drift in the clock's timing of TouchStar.

All electronic systems would have some inherent drift in its clock's timing. The term, drift, is referring to the difference between the electronic clock's time and that of a very accurate source.

While the clock of TouchStar has been designed to have as little drift as possible, the drift may inevitably become significant especially over a long period of time or under different temperature conditions.

As the drift accumulates, it may become significant to your application. For example, if the clock in TouchStar is faster than the accurate source by about 1 second per day, over a period of two months, it would grow to be faster by a minute.

As such, TouchStar has thus been designed to cater for such drift compensation.

How to get to menu:

Go to CONFIG → Clock (1st page) → Drift.

CLOCK DRIFT	
ADJUSTMENT(SECS) : +01	
SEL	EXIT
ENTER	

Description:

	Setting	Purpose	Available Selections
1	ADJUSTMENT(SECS)	<p>To set the amount of seconds to compensate the clock drift per day.</p> <p>The compensation can be “adjust forward” (+) or “adjust backward” (-).</p> <p>For example, “+01” means that the clock's time would be adjusted forward by 1 second per day.</p>	<p>The duration for adjustment ranges from 0 to 99 secs.</p> <p>(0 secs means there is no compensation at all.)</p>

How to change the settings:

- 1) Use the SEL key to change the direction of adjustment. That is, whether “+” or “-”.
- 2) Press the ENTER key to move the selection to the next digit. Use the SEL key next to toggle the digit.
- 3) When the settings are completed, press EXIT to save.

Remarks:**a) Finding out the number of seconds and the direction to compensate:**

First, set the clock's time with reference to an accurate source. Neutralize any compensation. In other words, the clock drift setting should be 0 seconds.

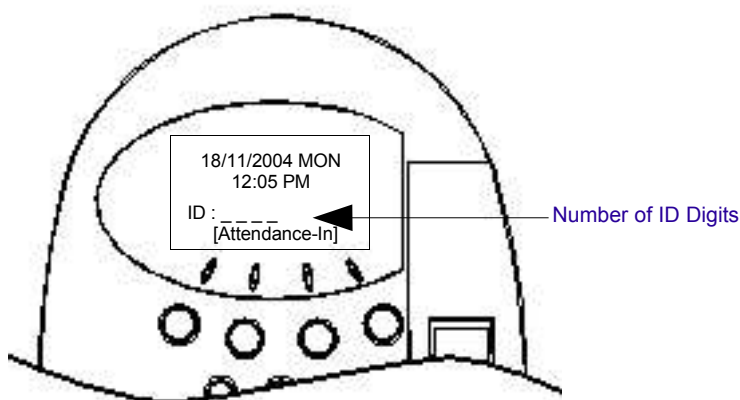
Monitor the clock's time again after a period of 5 or more days. Find out the difference between the clock's time and that of the accurate source. Divide the difference by the number of days monitored. You should now be able to know the number of seconds to compensate by day, and whether to compensate in the forward direction or the backward direction.

Notes:

Usually, you should not need to adjust the drift settings here. This is because it has already been preset in the factory before the device reaches to you. Only when you notice that there is some significant drift difference, then you may like to adjust the settings.

b. Setting the Number of ID Digits

The number of ID digits setting affects the number of digits that the user would need to key in at the User Page in order to do a one-to-one fingerprint verification. It also affects the number of digits that TouchStar would read from the contactless card.



Number of ID digits at the User Page

How to get to menu:

Go to CONFIG → Misc 1 (2nd page).

MISC 1 SETTING	
SETTING :	DEFAULT
NUMBER OF DIGITS :	4
FAIL WIEGAND OUT :	NO
SEL	EXIT
ENTER	

Description:

	Setting	Purpose	Available Selections
1	NUMBER OF DIGITS	To change the number of ID digits.	3 to 10

How to change the settings:

- 1) If SETTING is at [DEFAULT], use the SEL key to change it to [CUSTOMIZE].
- 2) Press the ENTER key to move the cursor to the NO. OF DIGITS row. Use the SEL key next to toggle the digit to the desired value.
- 3) Press EXIT to save.

c. Setting the Fail Wiegand Out Option

The Failed Wiegand Out option is a setting that allows TouchStar to send out reserved Wiegand codes upon a failed authentication. In order to use this feature, the receiving door controller needs to be able to understand the codes that are being sent out. The application of this feature is for systems that need to track the failed attempts through their external door controller.

How to get to menu:

Go to CONFIG → Misc 1 (2nd page).

MISC 1 SETTING	
SETTING	: [DEFAULT]
NUMBER OF DIGITS	: 4
FAIL WIEGAND OUT	: NO
SEL	EXIT
	ENTER

Description:

	Setting	Purpose	Available Selections
1	FAIL WIEGAND OUT	To enable or disable the sending out of special Wiegand ID codes when authentications fail.	YES / NO

How to change the settings:

- 1) If SETTING is at [DEFAULT], use the SEL key to change it to [CUSTOMIZE].
- 2) Press the ENTER key to move the cursor to the required row. Use the SEL key next to toggle the FAIL WIEGAND OUT setting to YES.
- 3) Press EXIT to save.

Remarks:**a) Codes being sent out upon a failed authentication:**

0001 – User ID is valid but fingerprint authentication failed.
 0002 – User ID does not exist.

d. Configuring the External Input Detect

TouchStar can be configured to wait for an acknowledgment signal from an external controller to ascertain that the Wiegand data it sent out previously upon a successful authentication had been properly received. If it does not receive the acknowledgment signal, it would display a message at the User Page to warn the user.

The External Input Detect setting here is meant for you to enable or disable this feature. If this feature is enabled, the setting also expects you to configure the duration of time that TouchStar should wait for the acknowledgment signal.

How to get to menu:

Go to CONFIG → Ext. In (2nd page).

EXTERNAL INPUT	
SETTING	: [CUSTOMIZE]
ENABLE	: WIEGAND ACK
TIMEOUT(SECS)	: 2.0
SEL	EXIT
	ENTER

Description:

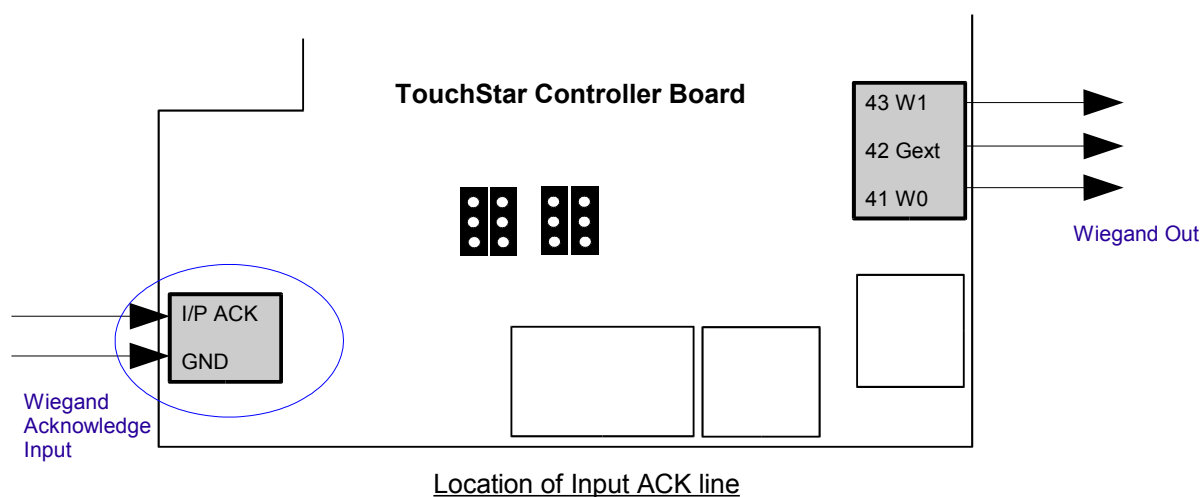
	Setting	Purpose	Available Selections
1	ENABLE	To select the type of usage for External Input Detect. Only WIEGAND ACK can be selected.	WIEGAND ACK only
2	TIMEOUT	To set the number of seconds that TouchStar would wait for the acknowledgment signal.	1.0 to 6.0 secs (in intervals of 0.5 secs)

How to change the settings:

- 1) If SETTING is at [DEFAULT], use the SEL key to change it to [CUSTOMIZE].
- 2) Press the ENTER key to move the cursor to the next row. Use the SEL key next to toggle the ENABLE setting from NO to WIEGAND ACK. When the setting is changed to WIEGAND ACK, the TIMEOUT row appears.
- 3) Use the ENTER key to move the cursor to the next row.
- 4) Use the SEL key to change TIMEOUT to the desired value.
- 5) Press EXIT to save the settings.

Remarks:**a) The Input ACK line is used for External Input Detect:**

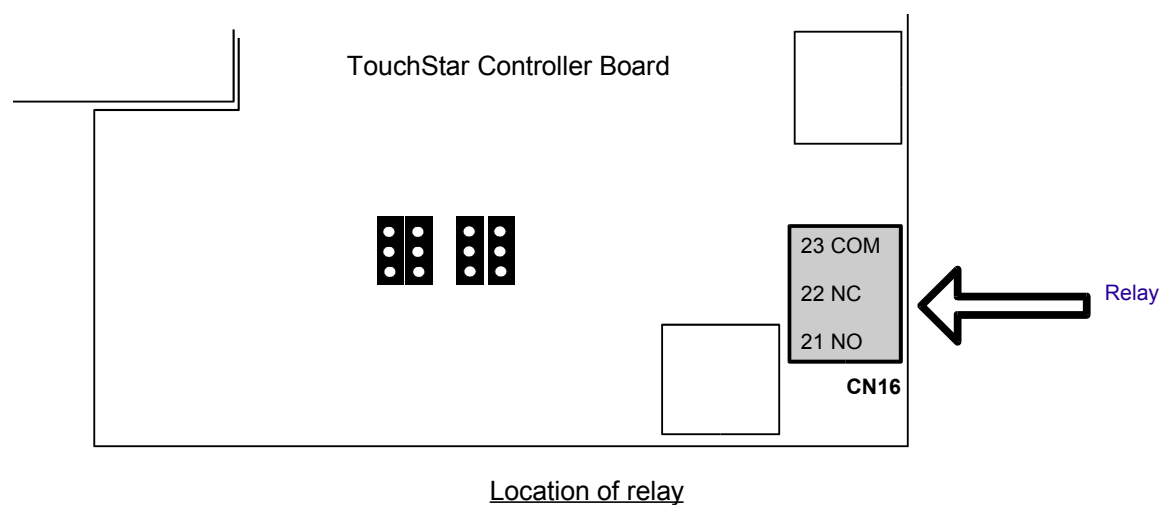
In order to use the Wiegand acknowledge signal, the signal from the external controller should be connected to the I/P – ACK pin. The signal should be a dry active-low signal.

**b) If the Wiegand Acknowledge is not received:**

If the Wiegand acknowledge signal is not received (upon a successful authentication) within the timeout duration, the message, “Validate Fail” would be flashed across the User Page. This informs you that the external controller had not sent back any acknowledgment to indicate that it has received the Wiegand output signal.

e. Configuring the Relay Option

TouchStar has an on-board relay that can be used for a few purposes. It can be used to trigger a bell, trigger a turnstile, or light up a lamp upon a successful authentication. It can also be used to ring the bell at fixed times.



How to get to menu:Go to CONFIG → Relay (2nd page).

SET RELAY TYPE	
SELECT →	DISABLE
SEL	EXIT ENTER

Description:

	Setting	Purpose	Available Selections
1	RELAY TYPE	To select the function of the relay.	a) DISABLE – The relay is not used for any function. b) ENABLE – The relay is used for activating a light, chime or door (See Notes) when authentication passes. c) BELL – The relay is used for activating a siren or bell at predefined timings. There are 2 types of predefined timings. One of them (Local Timings) can be set from the device; the other (Schedule 99), which is more flexible, can only be configured from the host software.

How to change the settings:

- 1) If you wish to change SELECT from DISABLE to ENABLE or BELL, use the SEL key.
- 2) When the desired mode has been selected, press the ENTER key to enter into more detailed settings for the selected setting. The details are described under **Remarks**.

Remarks:**a) Menu for ENABLE:**

If you have selected ENABLE, you would see the following display:

CONFIG RELAY	
SETTING :	DEFAULT
DURATION(SECS) :05	
SEL	EXIT ENTER

	Setting	Purpose	Available Selections
1	DURATION	To set the duration at which the relay remains triggered. For example, if you connect the relay to a chime, the chime would ring for the duration at which you set.	0 to 99 secs

In order to change the duration, first use the SEL key to change SETTING from DEFAULT to CUSTOMIZE. After this has been done, use the ENTER key to move the cursor and the SEL key to change the value.

To save the settings, press the EXIT key.

Notes:

The use of the relay to directly control an electromagnetic lock is not really recommended. For a more secure installation, the use of the TouchStar Door Zone Controller, or any external door controller from a third party vendor is advised.

b) Menu for BELL:

If you have selected BELL, you would see the following display:

SET BELL TYPE

SELECT → **LOCAL TIMING**

SEL
EXIT

ENTER

There are 2 selections for the bell type described as follows:

	Setting	Purpose	Available Selections
1	BELL TYPE	To select whether the bell should ring based on timings that can be configured directly on the device (Local Timings), or based on a set of schedule (Schedule 99, or known as Bell Schedule).	a) LOCAL TIMING b) SCHEDULE 99

Press SEL to toggle the selection. When the selection has been selected, press ENTER to get into the detailed settings for that selection.

i) Local Timing:

If you have selected LOCAL TIMING, you would see the following display:

SET LOCAL BELL

BELL 1

BELL 2
BELL 3
BELL 4
BELL 5

OK
EXIT
BACK
FWD

There are a total of 20 local bell timings that can be used. Use the OK key to enter the detailed settings for the selected bell. To scroll through the various bells, use the BACK or FWD keys.

When the OK key is pressed for the selected bell, you would see the following display:

```

CONFIG BELL 1
BELL      : ON
DURATION(SECS) : 05

01:00 PM

SEL  EXIT  ENTER

```

To enable this bell, use the SEL key to toggle OFF to ON. Next use the ENTER key to move the cursor to change the duration or the bell's time. To save the settings, press EXIT.

When this bell is enabled, an "ON" status would be reflected against it as shown below.

```

SET LOCAL BELL
BELL 1  ON
BELL 2
BELL 3
BELL 4
BELL 5
OK  EXIT  BACK  FWD

```

You can repeat these steps for other bells.

ii) Schedule 99 (Bell Schedule):

If you have selected LOCAL TIMING, you would see the following display:

```

SET SCH99 BELL
SETTING : [DEFAULT]
DURATION(SECS) : 05

SEL  EXIT  ENTER

```

	Setting	Purpose	Available Selections
1	DURATION	To set the duration at which the relay remains triggered.	0 to 99 secs

In order to change the duration, first use the SEL key to change SETTING from DEFAULT to CUSTOMIZE. After this has been done, use the ENTER key to move the cursor and the SEL key to change the value.

To save the settings, press the EXIT key.

c) Difference between Local Timing and Schedule 99:

When you set the bells using Local Timing, the bell timings apply to all the seven days in the week. However, with Schedule 99, you would be able to configure the bells more flexibly. For example, you would be able to ring the bell at 8.00pm on the weekdays, while at 9.00pm on Saturdays and Sundays.

f. Selecting the Language

Only the English language is supported in TouchStar. The menus throughout the device are displayed in English. However, when you change the LANGUAGE setting to SPANISH, although the menus remain in English, the following displays at the User Page are changed. In other words, only a limited part is translated to Spanish.

In English	In Spanish
1. Mon	Lun
2. Tue	Mar
3. Wed	Mie
4. Thu	Jue
5. Fri	Vie
6. Sat	Sab
7. Sun	Dom
8. Welcome	Bienvenido

How to get to menu:

Go to CONFIG → Language (3rd page).

LANGUAGE	
SETTING	: [DEFAULT]
SELECT	: ENGLISH
<div> <div>SEL</div> <div>EXIT</div> <div></div> <div>ENTER</div> </div>	

Description:

	Setting	Purpose	Available Selections
1	SELECT	To change the language.	a) ENGLISH b) SPANISH

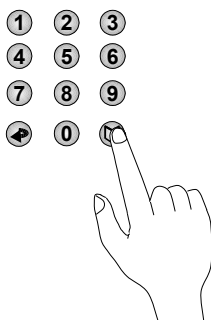
How to change the settings:

- 1) If SETTING is at [DEFAULT], use the SEL key to change it to [CUSTOMIZE].
- 2) Press the ENTER key to move the cursor to the next row. Use the SEL key next to toggle the setting to the desired value.
- 3) Press EXIT to save.

g. Selecting the Time Attendance Field Descriptor Set

The Time Attendance Field Descriptor is the description that appears at the bottom part of the TouchStar screen. Depending on what is displayed, the log that is recorded upon a passed authentication would carry the log type that is associated with this description.

TouchStar supports a few sets of the field descriptors. When a particular set has been selected, the fields within the selected set can be toggled by pressing the Attendance Mode key.



Pressing the Attendance Mode key to change the field descriptor

How to get to menu:

Go to CONFIG → T/A (3rd page).

ATTD DISPLAY	
SETTING	: [DEFAULT]
SELECT	: WELCOME
<div> <div>SEL</div> <div>EXIT</div> <div></div> <div>ENTER</div> </div>	

Description:

	Setting	Purpose	Available Selections
1	SELECT	To change the time attendance field descriptor set.	a) WELCOME b) ATTD/ACCESS c) ATTD/ACCESS V1 d) ATTD (2 LEVELS) e) ATTD (6 LEVELS) f) ATTD (7 LEVELS) g) ATTD/ACCESS V2

How to change the settings:

- 1) If SETTING is at [DEFAULT], use the SEL key to change it to [CUSTOMIZE].
- 2) Press the ENTER key to move the cursor to the next row. Use the SEL key next to toggle the setting to the desired value.
- 3) Press EXIT to save.

Remarks:

The fields for each descriptor set are tabulated in the table below. For example, if you choose ATTD (2 LEVELS), the “In” field is associated with log type 1, while the “Out” field is associated with log type 2.

Table of Field Descriptors:

Log Type	Field Descriptor Set						
	(a) Welcome	(b) Attd/Access	(c) Attd/Access V1	(d) Attd (2 Levels)	(e) Attd (6 Levels)	(f) Attd (7 Levels)	(g) Attd/Access V2
1	Welcome	Attendance		In	Attendance-In	Waktu Masuk	In
2		Access Control	Access Control	Out	Leaving-Out	Waktu Keluar	Out
3					Early Leave	Hujan	Access Control
4					Going Out	Hospital	
5					Return	Jalan Sesak	
6					Others	Kndrn Rosak	
7			In			Anak Sakit/Skl	
8			Out				

h. Selecting the Auxiliary Device

The Auxiliary Device setting refers to the type of contactless card reader that is fitted within TouchStar (other than the HID card reader). The type of auxiliary devices supported in TouchStar are:

- 1) Mifare reader
- 2) Bar Code reader
- 3) Magnetic Strip reader

If none of these readers are fitted within TouchStar, this setting should not be made.

How to get to menu:

Go to CONFIG → Aux Dev (3rd page).

AUX INPUT DEVICE

SELECT → DISABLE

SEL
EXIT
ENTER

Description:

	Setting	Purpose	Available Selections
1	SELECT	To select the type of auxiliary device used.	a) DISABLE b) MIFARE c) BAR CODE d) MAGNETIC

How to change the settings:

- 1) Use the SEL key to toggle the selection to the desired setting (other than DISABLE).
- 2) Once the desired setting has been selected, if you want to save the selected auxiliary device, you can press the EXIT key. (For the Mifare reader, if the reader is not detected, you would not be able to save.)
- 3) If you would like to go into more detailed settings for this selection, press the ENTER key. The detailed settings are shown in **Remarks**.

Remarks:**a) Menu for MIFARE:**

If you have selected MIFARE, you would see the following menu. This menu allows you to test out the reading of the Mifare card.

Press ENTER to go into the Test selection.

MIFARE READER			
Test			
SE I	EXIT		ENTER

Under the Test selection, you would be able to flash the Mifare card across the device and test out whether the reader is reading the card properly

READ MIFARE CARD

b) Menu for BAR CODE:

If you have selected BAR CODE, you would see the following menu. This menu also allows you to test out the reading of the bar coded card.

Press ENTER to go into the Test selection.

BAR CODE READER	
Test	
SE	EXIT
	ENTER

Under the Test selection, you would be able to swipe the bar coded card across the bar code reader and test out whether the reader is reading the card properly

READ BAR CODE	
Please scan card	
	EXIT

c) Menu for MAGNETIC:

If you have selected MAGNETIC, you would see the following menu. Press ENTER to go into the Setup selection.

MAGNETIC READER	
Setup	
Test	
SE	EXIT
	ENTER

Under the Setup selection, you can setup TouchStar to read the desired information from the magnetic strip card. The desired information is located by the Track Number and the Field Number.

MAGNETIC SETUP	
SETTING :	DEFAULT
TRACK NUMBER :	2
FIELD NUMBER :	1
<div> <div>SEL</div> <div>EXIT</div> <div></div> <div>ENTER</div> </div>	

	Setting	Purpose	Available Selections
1	TRACK NUMBER	To set the track number of the magnetic strip where the desired information resides.	1 to 3
2	FIELD NUMBER	Each track has a few fields. This selection allows you to select the specific field where the information resides.	1 to 5

Please consult your dealer for the proper settings if you are unsure.

To change the settings, use the SEL key to change SETTING from DEFAULT to CUSTOMIZE. Next, use the ENTER key to move the selection to the next few rows. Use the SEL key to toggle until the desired value is obtained. To save the settings, press the EXIT key.

Next, you can test out the reading of the card by selecting Test from the previous menu.

i. Enabling or Disabling the Numeric Keys

The numeric keys refer to the keys labeled with the digits 0 to 9. These keys are enabled by default. This means that you can always make use of the keys to enter the User ID so that you can perform an authentication. However, you can choose to disable these keys to prevent the user from making a keyed input. One use of this feature is that you would like to enforce a policy where the users must make use of their cards to provide the User ID to perform an authentication. The following describes how the numeric keys can be disabled.

How to get to menu:

Go to CONFIG → Verify (3rd page).

VERIFY OPTIONS	
SETTING :	DEFAULT
NUMERIC KEYS :	ENABLE
HIDE CARD ID :	DISABLE
<div> <div>SEL</div> <div>EXIT</div> <div></div> <div>ENTER</div> </div>	

Description:

	Setting	Purpose	Available Selections
1	NUMERIC KEYS	To enable or disable the numeric keys.	ENABLE / DISABLE

How to change the settings:

- 1) If SETTING is at DEFAULT, use the SEL key to toggle it to CUSTOMIZE.
- 2) Use the ENTER key to move the cursor to the NUMERIC KEY row.
- 3) Use the SEL key to toggle NUMERIC KEYS to either ENABLE or DISABLE, depending on which is your desired input.
- 4) Press EXIT to save the settings.

Notes:

If NUMERIC KEYS is set to DISABLE, the 4 Function keys, the Erase key and the Attendance Mode key still remains enabled.

j. Displaying or Hiding the Card ID

When the card is flashed across the device, the Card ID is displayed at the User Page. If you would like to hide the Card ID from displaying so that the users are prevented from knowing their Card IDs, you can enable this feature.

When you choose to hide the Card ID, the User Page displays a series of “ * ” as replacement for the Card ID.

How to get to menu:

Go to CONFIG → Verify (3rd page).

VERIFY OPTIONS	
SETTING :	DEFAULT
NUMERIC KEYS :	ENABLE
HIDE CARD ID :	DISABLE
SEL	EXIT ENTER

Description:

	Setting	Purpose	Available Selections
1	HIDE CARD ID	To either hide the Card ID, or allow it to be displayed when it is flashed at the device.	ENABLE / DISABLE

How to change the settings:

- 1) If SETTING is at DEFAULT, use the SEL key to toggle it to CUSTOMIZE.
- 2) Use the ENTER key to move the cursor to the NUMERIC KEY row.
- 3) Use the SEL key to toggle HIDE CARD ID to either ENABLE or DISABLE, depending on which is your desired input.
- 4) Press EXIT to save the settings.

k. Setting the Multiple Fingerprint Verification Option

The Multiple Fingerprint Verification option is disabled by default. When it is enabled, it can be set to 2 or 3 fingerprints verification. What this means is that if it is set to 2, two fingerprints belonging to the same User ID must be matched before the matching can be considered as successful.

How to get to menu:

Go to CONFIG → FP Auth (4th page).

CONFIG FP AUTH	
SETTING :	DEFAULT
ALLOW KEYPAD INPUT	
AS CARD INPUT	: NO
MULTIPLE FP	: 1
SEL	EXIT ENTER

Description:

	Setting	Purpose	Available Selections
1	MULTIPLE FP	To set the number of fingerprints to be verified successfully before authentication is considered as passed.	1, 2 and 3.

How to change the settings:

- 1) If SETTING is at DEFAULT, use the SEL key to toggle it to CUSTOMIZE.
- 2) Use the ENTER key to move the cursor to the MULTIPLE FP row.
- 3) Use the SEL key to toggle MULTIPLE FP to 1, 2 or 3 depending on which is your desired input.
- 4) Press EXIT to save the settings.

Notes:

1. If MULTIPLE FP is set to 3 for example, each user record must be enrolled with at least 3 fingerprints. Otherwise, authentication would be rejected for this user.
2. Identification (one-to-many matching) and Speed Search are automatically disabled when MULTIPLE FP is set to 2 or 3.

I. Allowing Keypad Input to Replace Card Input for Fingerprint Verification

When you enroll a user with fingerprint, you may use the keypad to provide the User ID, or you may use a card scan to provide the User ID. If you have used the card scan to provide the User ID, during matching, if you try to use the keypad to enter this ID, you would be prevented from continuing with the fingerprint matching. This is because the card is treated as an additional authentication factor, and must be present for a record that was enrolled together with it.

The need for the card to be present for such records can be done away with by turning on this feature. In other words, when this feature is enabled, for a fingerprint record that was enrolled together with a card, you can still use the keypad to provide the ID.

By turning on this feature, you also allow the one-to-many search and Speed Search operations to search through these records as well.

How to get to menu:

Go to CONFIG → FP Auth (4th page).

CONFIG FP AUTH	
SETTING :	DEFAULT
ALLOW KEYPAD INPUT	
AS CARD INPUT	: NO
MULTIPLE FP	: 1
SEL	EXIT
	ENTER

Description:

	Setting	Purpose	Available Selections
1	ALLOW KEYPAD INPUT AS CARD INPUT	To allow the keypad to be used to provide the User ID for fingerprint records that were previously enrolled together with card scan.	YES / NO

How to change the settings:

- 1) If SETTING is at DEFAULT, use the SEL key to toggle it to CUSTOMIZE.
- 2) Use the ENTER key to move the cursor to the ALLOW KEYPAD INPUT AS CARD INPUT row.
- 3) Use the SEL key to toggle ALLOW KEYPAD INPUT AS CARD INPUT to YES or NO depending on which is your desired input.
- 4) Press EXIT to save the settings.

m. Allowing Keypad Input to Replace Card Input for PIN Verification

When you enroll a user with PIN, you may use the keypad to provide the User ID, or you may use a card scan to provide the User ID. If you have used the card scan to provide the User ID, during matching, if you try to use the keypad to enter this ID, you would be prevented from continuing with the PIN matching. This is because the card is treated as an additional authentication factor, and must be present for a record that was enrolled together with it.

The need for the card to be present for such records can be done away with by turning on this feature. In other words, when this feature is enabled, for a PIN record that was enrolled together with a card, you can still use the keypad to provide the ID.

How to get to menu:

Go to CONFIG → PIN Auth (4th page).

CONFIG PIN AUTH	
SETTING	: DEFAULT
PIN ONLY	: NO
NO. OF PIN DIGITS	: 6
<div> <div>SEL</div> <div>EXIT</div> <div></div> <div>ENTER</div> </div>	

Description:

	Setting	Purpose	Available Selections
1	PIN ONLY	To allow the keypad to be used to provide the User ID for PIN records that were previously enrolled together with card scan.	a) NO - Keypad input cannot be used to replace card input. b) YES – Keypad input can be used to replace card input.

How to change the settings:

- 1) If SETTING is at DEFAULT, use the SEL key to toggle it to CUSTOMIZE.
- 2) Use the ENTER key to move the cursor to the PIN ONLY row.
- 3) Use the SEL key to toggle PIN ONLY to YES or NO depending on which is your desired input.
- 4) Press EXIT to save the settings.

n. Setting the Number of PIN Digits

For PIN matching, the user has to key in their PIN after providing the User ID. The number of PIN digits is 6 by default. However, you can also change the number of digits to 4 or 5.

How to get to menu:

Go to CONFIG → PIN Auth (4th page).

CONFIG PIN AUTH	
SETTING :	DEFAULT
PIN ONLY :	NO
NO. OF PIN DIGITS :	6
<div> SEL EXIT ENTER </div>	

Description:

	Setting	Purpose	Available Selections
1	NO. OF PIN DIGITS	To set the number of digits for PIN entry	4 to 6.

How to change the settings:

- 1) If SETTING is at DEFAULT, use the SEL key to toggle it to CUSTOMIZE.
- 2) Use the ENTER key to move the cursor to the NO. OF PIN DIGITS row.
- 3) Use the SEL key to toggle NO. OF PIN DIGITS to 4, 5 or 6 depending on which is your desired input.
- 4) Press EXIT to save the settings.

5.1.3 Inside the LOG Page

a. Setting the Duplicate Check Option

The Duplicate Check option is a feature that checks for any log records in the device with the same User ID, and prevent further logging when it is found. When you choose to enable this feature, you would be asked to provide the time frame to check on. For example, if you specify 10 minutes, the device would search for such log records from the time you perform the authentication back to 10 minutes ago.

If a log record is found within this time frame, a new log would not be created. The User Page would display the message, “Already Logged” to alert you.

How to get to menu:

Go to LOG → DUP CHK.

DUPLICATE CHECK	
SETTING :	CUSTOMIZE
ENABLE CHECK :	YES
INTERVAL(MIN) :	30
SEL	EXIT
	ENTER

Description:

	Setting	Purpose	Available Selections
1	ENABLE CHECK	To enable or disable duplicate check.	YES / NO
2	INTERVAL(MIN)	The time frame at which duplicate check would check up to.	1 to 99

How to change the settings:

- 1) If SETTING is at DEFAULT, use the SEL key to toggle it to CUSTOMIZE.
- 2) Use the ENTER key to move the cursor to the ENABLE CHECK row.
- 3) Use the SEL key to toggle ENABLE CHECK to YES or NO depending on which is your desired input.
- 4) If you have selected YES to the above, you can adjust the INTERVAL.
- 5) After INTERVAL has been adjusted, press EXIT to save the settings.

Notes:

During the duplicate check operation, only the Time Attendance (or transaction) log records are searched. The Event traces, Failed Attempts logs and Authentication Mode traces are not searched.

b. Enabling or Disabling Event Trace, Failed Attempts and Authentication Mode Trace Logs

There are 4 types of log records:

- 1) Time Attendance (or transaction)
- 2) Event Trace
- 3) Failed Attempts
- 4) Authentication Mode Trace

These logs are explained in more details in "**Chapter 3.5 - Logging (page 16)**". By default, the last 3 types of log records are disabled. This means that whenever any related events are triggered, the relevant logs are not recorded any way. If you wish to enable any of these logs, you can follow the steps below.

How to get to menu:

Go to LOG → OPTIONS.

LOG OPTIONS	
SETTING	: [DEFAULT]
LOG TRACE	: NO
LOG FAIL ATTEMPT	: NO
LOG AUTH PROFILE	: NO
SEL	EXIT ENTER

Description:

	Setting	Purpose	Available Selections
1	LOG TRACE	To enable or disable Event trace logs.	YES / NO
2	LOG FAIL ATTEMPT	To enable or disable Failed Attempts logs.	YES / NO
3	LOG AUTH PROFILE	To enable or disable Authentication Mode trace logs.	YES / NO

How to change the settings:

- 1) If SETTING is at DEFAULT, use the SEL key to toggle it to CUSTOMIZE.
- 2) Use the ENTER key to move the cursor to the desired row.
- 3) Use the SEL key to toggle the setting to YES or NO depending on which is your desired input.
- 4) Repeat for other desired settings.
- 5) Press EXIT to save the settings.

Chapter 6

6 Setting Up for Communication

Communication with TouchStar is so important because if you are unable to communicate with it, you would not be able to configure the device remotely, or distribute the fingerprint templates from the application program to all the devices that the software controls. This chapter describes how you can connect the device to the host PC.

The description would be categorized into the following modes of communication that supported by TouchStar:

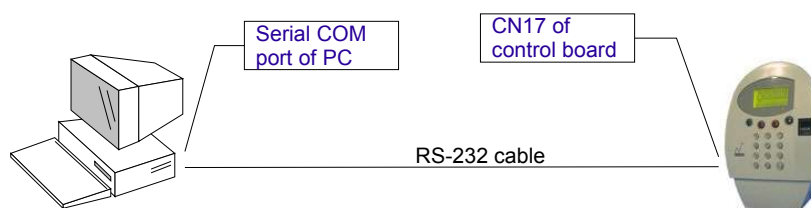
- 1) RS-232
- 2) RS-422 and RS-485
- 3) TCP/IP
- 4) Modem

6.1 Using RS-232

RS-232 is the simplest configuration among all the available modes of communication. However, it only supports a single device from a single communication port of the host computer.

Outline:

A serial RS-232 cable is used to connect the TouchStar device to the host computer. Use the cable that is supplied with your packaging.

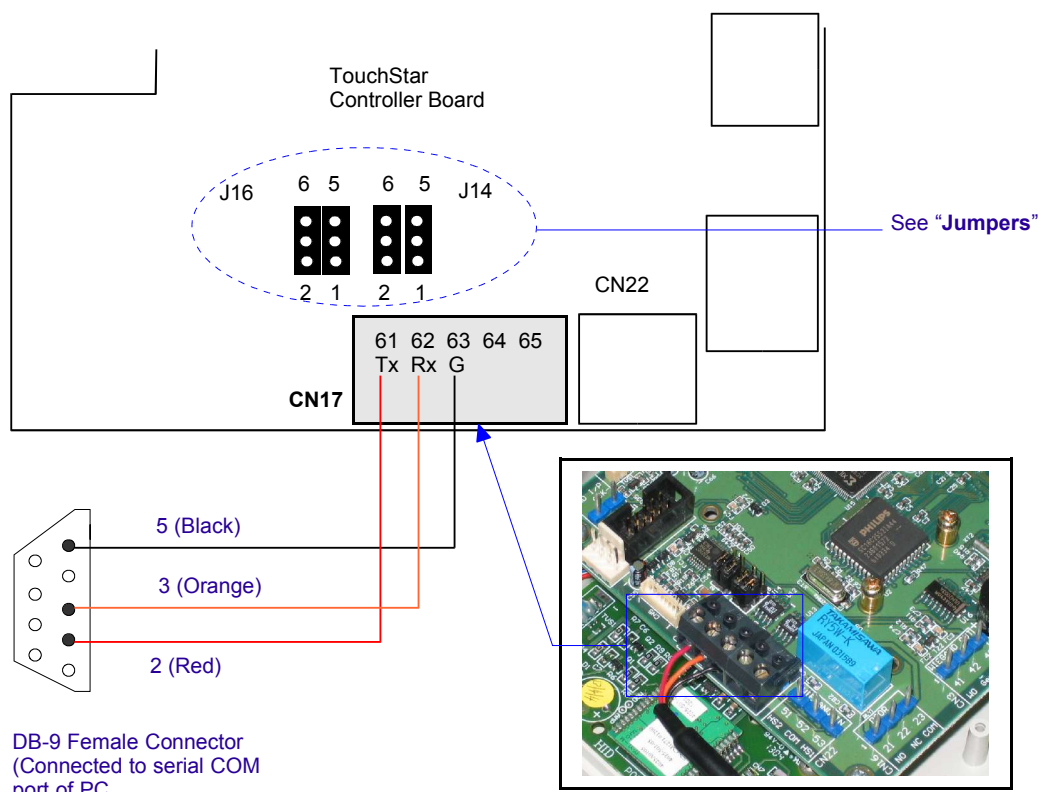


RS-232 Connection

Connection:

a) RS-232 Cable From Serial COM Port to TouchStar Controller Board

If you are using the serial RS-232 cable that comes with your packaging, it is connected to a screw terminal block with the color code illustrated below. Connect the block to CN17 of the TouchStar Controller Board. The other end should be connected to the serial COM port of the host computer.



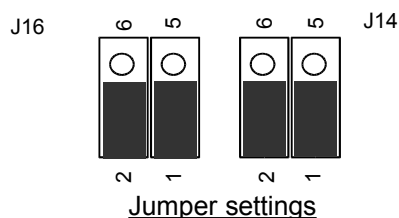
Pin-out:

DB-9 Connector (To PC)	TouchStar (CN17)
2 (Rx)	61 (Tx)
3 (Tx)	62 (Rx)
5 (Ground)	63 (G)

RS-232 cable pin-out from PC to TouchStar

Jumpers:

Connect the jumpers as shown below. All 4 jumpers should be at the lower position.



Menu Setting:

Follow the menu setting described in "**Chapter 4.2.5d - Setting the Communication Type (page 42)**".

Application Program Setting:

The Device ID and Baud Rate you choose under the menu described above should be the same as that in the application program.

6.2 Using RS-422 and RS-485

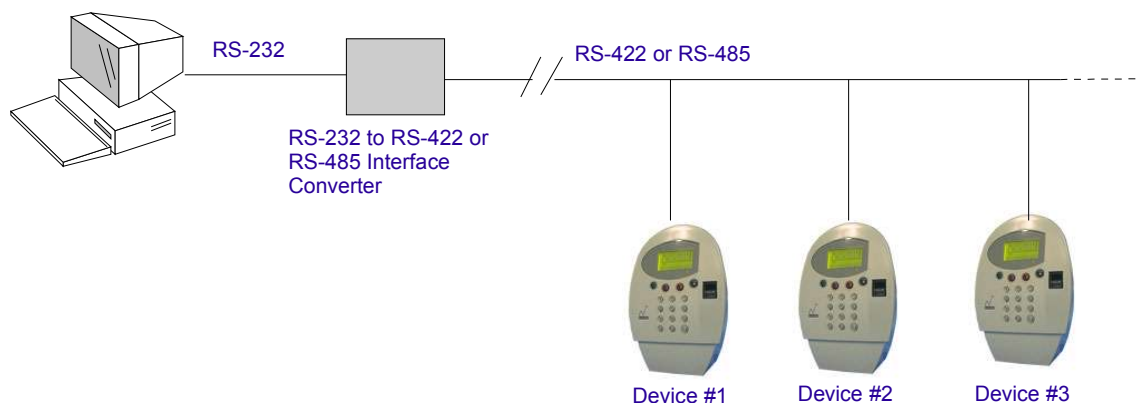
RS-422 and RS-485 allows several devices to be connected in a daisy-chain manner. The maximum line distance is also extended.

Outline:

If you are using RS-422 or RS-485, a RS-232 to RS-422 or RS-485 interface converter is required. This is because the signal from the PC is RS-232. With the converter, the signal would be converted to RS-422 or RS-485 before it is received by the devices.

If you are using the interface converter known as ADAM 4520, you can additionally refer to the following appendices :

- **Appendix E – ADAM 4520 RS-232 to RS-422 / 485 Interface Converter (page 99)**
- **Appendix F – Using the ADAM-4520 in RS-422 and RS-485 Communication (page 101)**

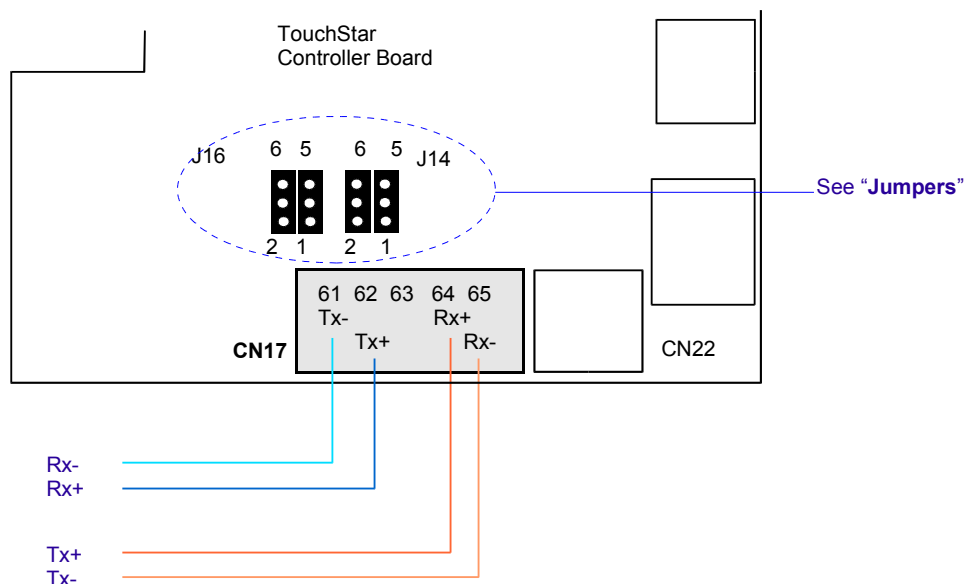


RS-422 or RS-485 daisy chain connection

6.2.1 RS-422

For RS-422, 4 wires are used.

Connection:



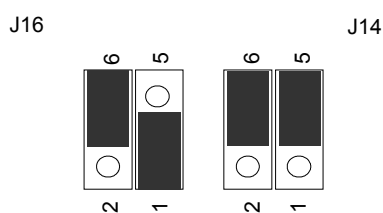
Pin-out:

Interface Converter	TouchStar (CN17)
Rx-	61 (Tx-)
Rx+	62 (Tx+)
Tx-	64 (Rx+)
Tx+	65 (Rx-)

RS-422 cable pin-out from Interface Converter to TouchStar

Jumpers:

Connect the jumpers as shown below.



Jumper Settings for RS-422

Menu Setting:

Follow the menu setting described in "**Chapter 4.2.5d - Setting the Communication Type (page 42)**".

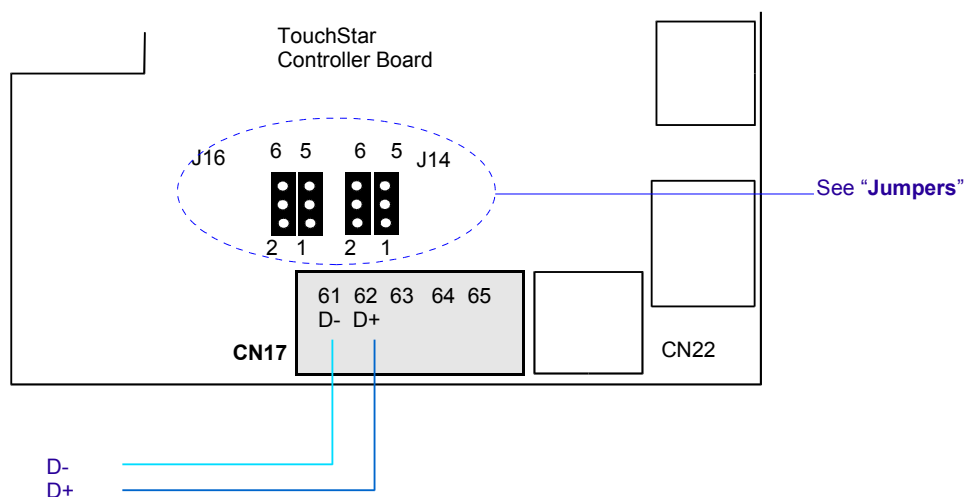
Application Program Setting:

The Device ID and Baud Rate you choose under the menu described above should be the same as that in the application program.

6.2.2 RS-485

For RS-485, 2 wires are used.

Connection:



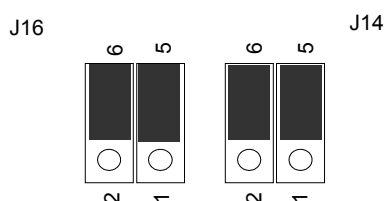
Pin-out:

Interface Converter	TouchStar (CN17)
D-	61 (D-)
D+	62 (D+)

RS-485 cable pin-out from Interface Converter to TouchStar

Jumpers:

Connect the jumpers as shown below. All jumpers are in the upper position.



Jumper Settings for RS-485

Menu Setting:

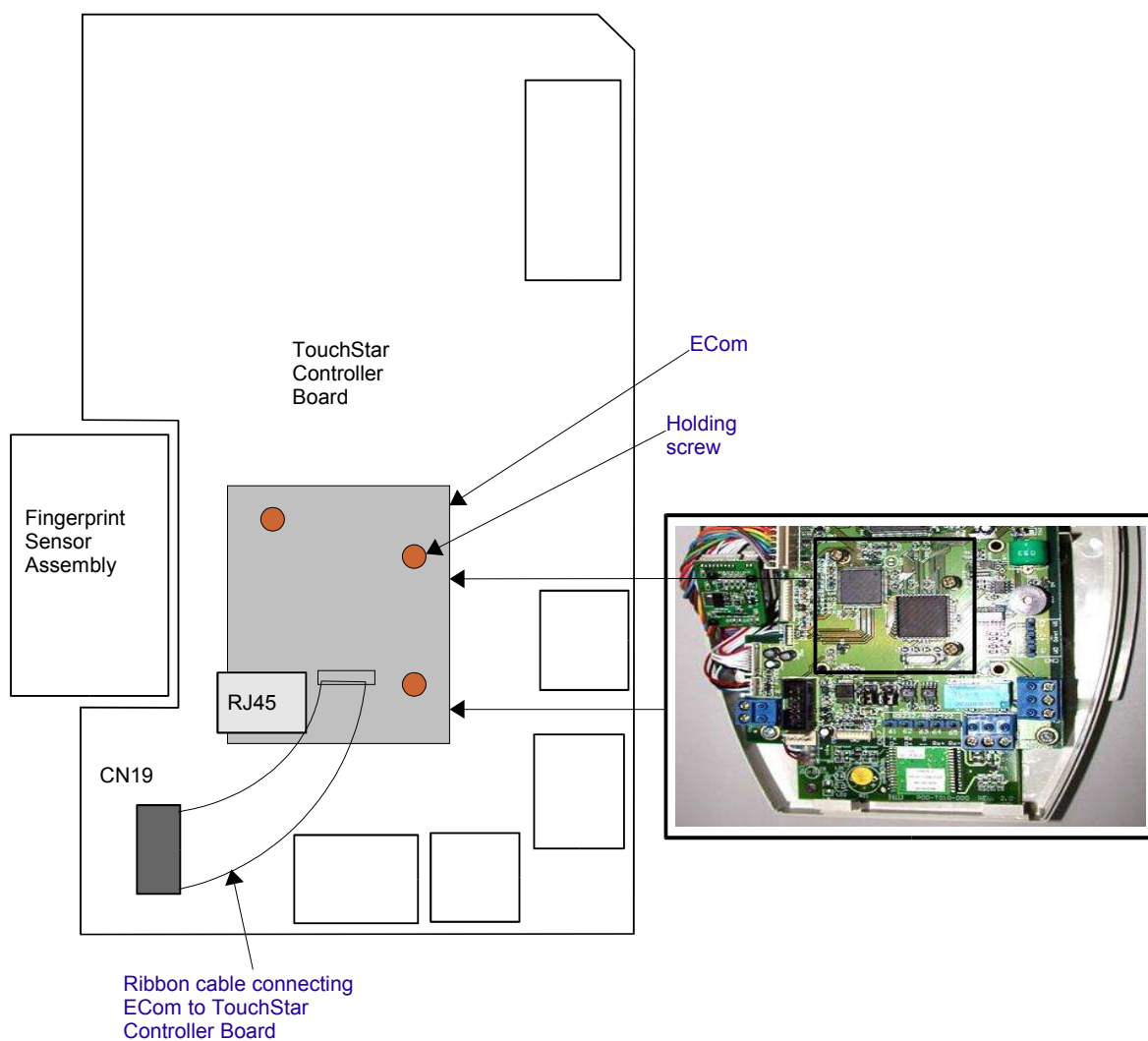
Follow the menu setting described in "**Chapter 4.2.5d - Setting the Communication Type (page 42)**".

Application Program Setting:

The Device ID and Baud Rate you choose under the menu described above should be the same as that in the application program.

6.3 Using TCP/IP

If you intend to communicate using TCP/IP, TouchStar must be fitted with an Ethernet add-on board. The following diagram shows how the Ethernet board (also known as ECom) is fitted onto the TouchStar Controller board.

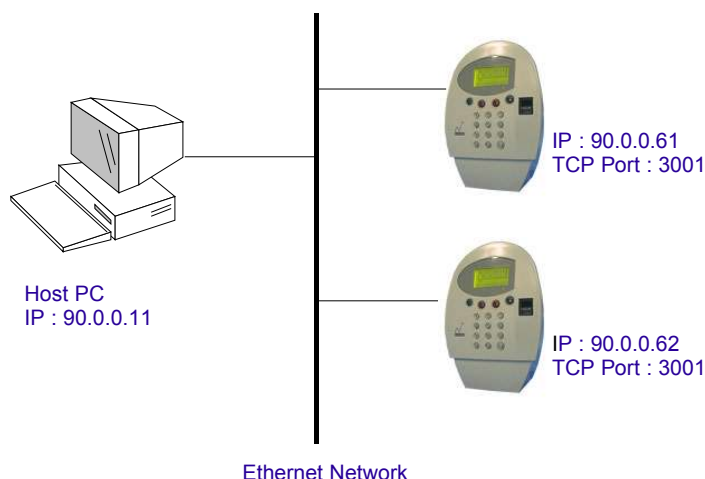


Picture of ECom

The ECom board is connected to the TouchStar controller board at CN19 using a ribbon cable. To secure the board to the main board, 3 holding screws are used as shown. Not shown in the above diagram, the ribbon cable is usually routed in such a way that most of it is beneath the main board. If too much of it is exposed above the main board, it may create some hindrance.

Outline:

The following diagram shows how TouchStar devices are connected to the network. Each device needs to be assigned with a static IP address. In addition, you need to assign a specific TCP Port number to each device.



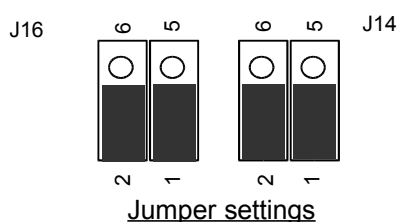
Ethernet Network

Connection:

Connect ECom to the CN19 of the TouchStar controller board using the ribbon cable provided.

Jumpers:

Connect the jumpers as shown below. All 4 jumpers should be at the lower position. If you notice, the position of the jumpers are similar to that in RS-232.



Menu Setting:

You would need to configure the IP address, Gateway address, Subnet Mask and TCP Port. Follow the menu setting described in "**Chapter 4.2.5d - Setting the Communication Type (page 42)**".

Application Program Setting:

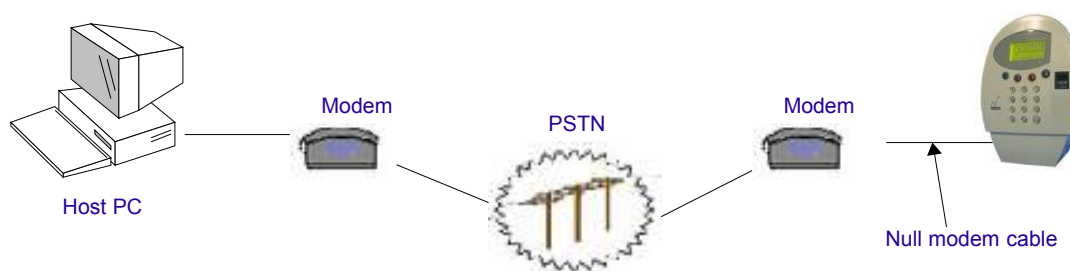
In the application program, the IP address and TCP Port number must be specified according to what have been configured in the device.

6.4 Using the Modem

Using the modem, you can communicate with a single TouchStar, or a number of TouchStar devices that have been daisy-chained together. While only external modems are supported, you may also use the proprietary internal modem supplied only by your local dealer. If the internal modem is used, one modem can only be used for one TouchStar device. The following diagrams show the two different types of connections.

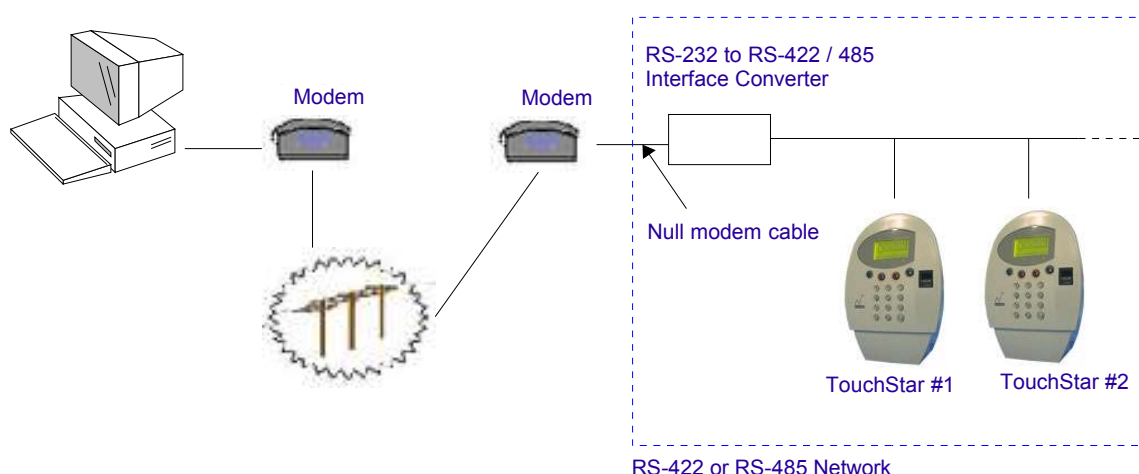
Outline:

If a single TouchStar device is to be used, the device is connected to the modem using a null modem cable. The layout of the null modem cable is described later.



Modem to single TouchStar device

If multiple TouchStar devices are to be used, a RS-232 to RS-422 / RS-485 interface converter is required. The converter is also connected to the modem using a null modem cable. However, this null modem cable is different from the one above. Notice that the TouchStar devices are actually connected together in a RS-422 or RS-485 network.



Modem to multiple TouchStar devices

Let us look at the specifics for each type of connection.

6.4.1 Single TouchStar

Connection:

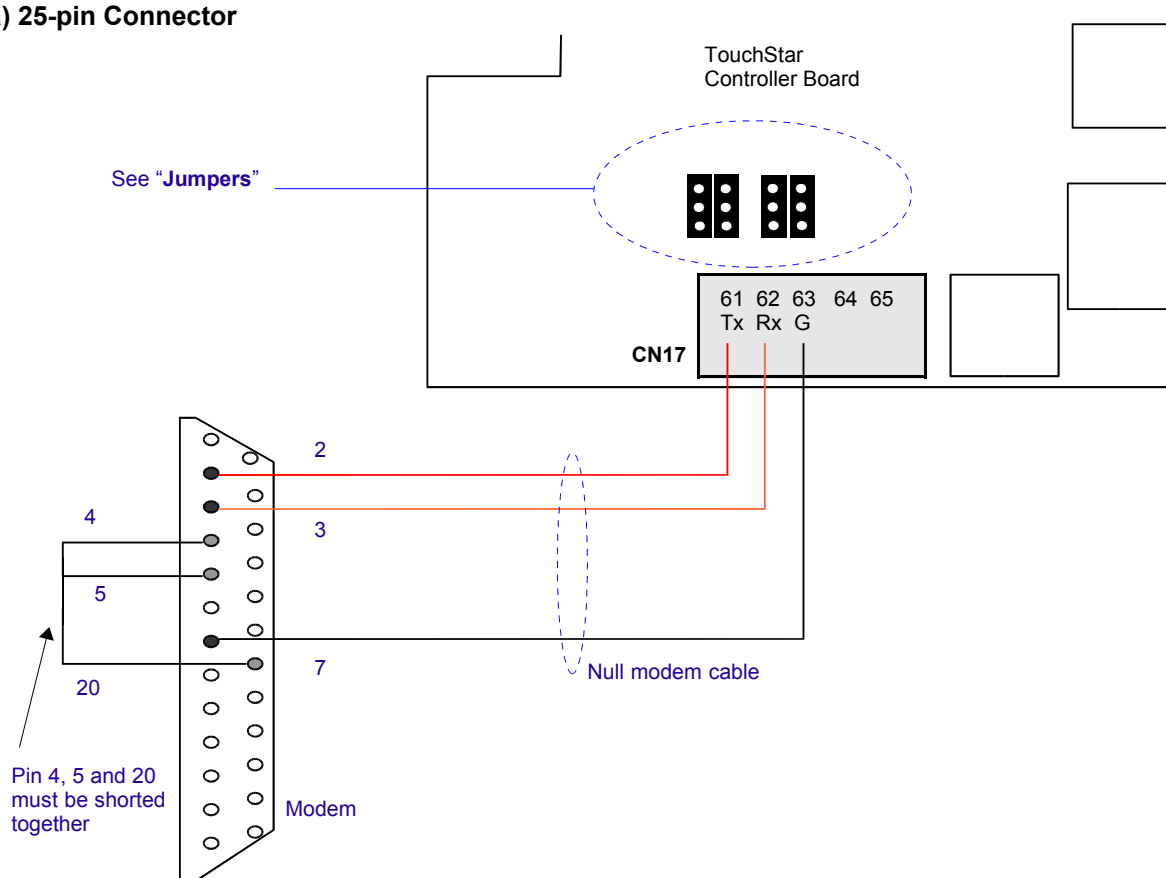
If an external modem is used, the modem is connected to the TouchStar using a null modem cable. You should not use the standard RS-232 cable that is supplied together with the packaging. Please consult your dealer for this cable. Alternatively, it can be created by yourself using the pin-out shown below.

Notes:

Do not use the standard RS-232 cable that is supplied together with your packaging to connect the modem to the TouchStar.

Depending on the type of modem you have, it may have a 9-pin DB connector, or a 25-pin DB connector. The one that is frequently used nowadays is the 25-pin.

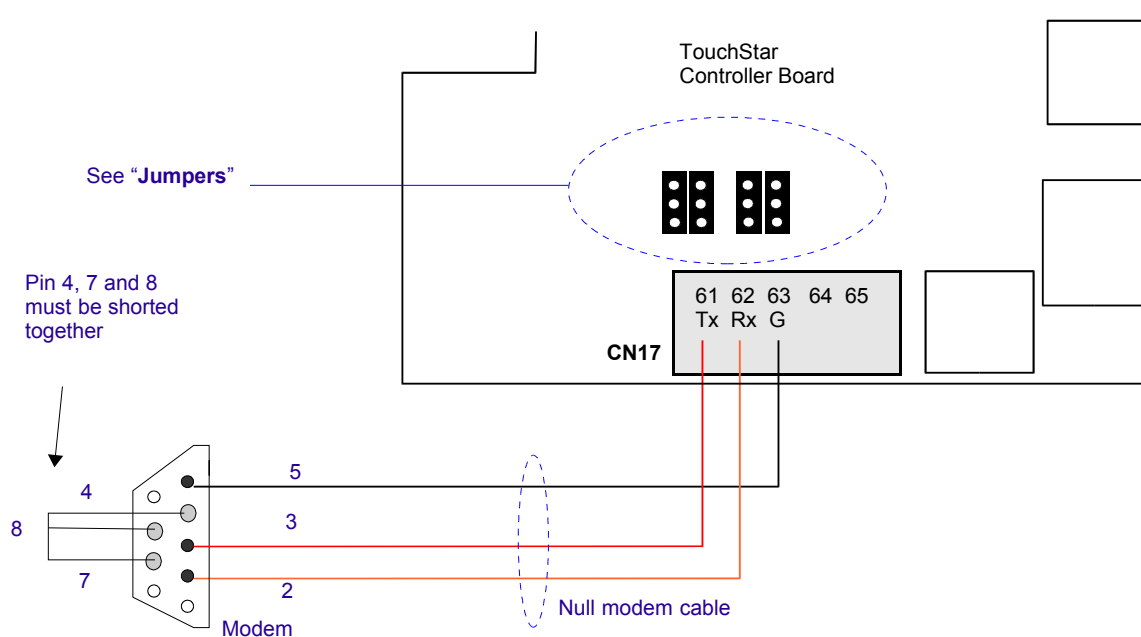
a) 25-pin Connector



Pin-out:

Modem	TouchStar (CN17)
2	61 (Tx)
3	62 (Rx)
7	63 (Ground)

Connecting a 25-pin modem to TouchStar

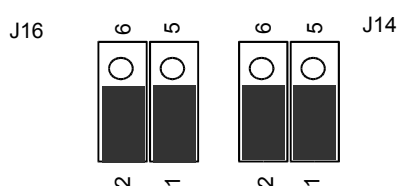
b) 9-pin Connector**Pin-out:**

Modem	TouchStar (CN17)
3	61 (Tx)
2	62 (Rx)
5	63 (Ground)

Connecting a 9-pin modem to TouchStar (Note that it is different from the 25-pin)

Jumpers:

For both 9-pin and 25-pin modems, the 4 jumpers are connected at the lower position as shown below.



Jumper settings

Menu Setting:

You would need to configure the Device ID and Baud Rate. Follow the menu setting described in "Chapter 4.2.5d - Setting the Communication Type (page 42)".

Application Program Setting:

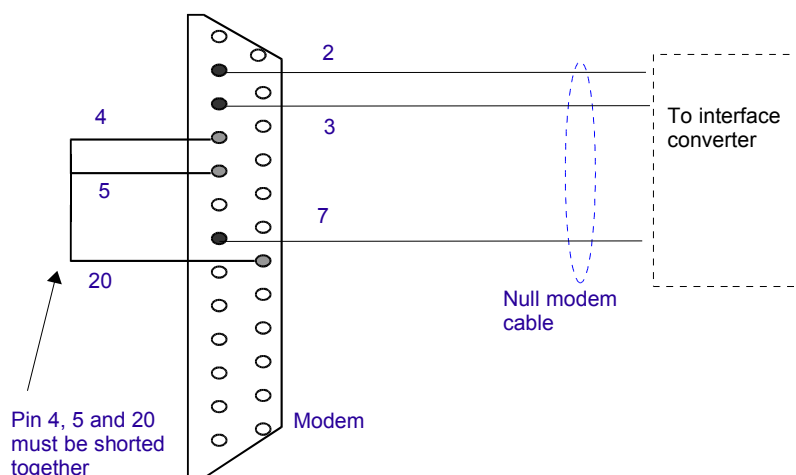
The Device ID you choose under the menu described above should be the same as that configured in the application program.

6.4.2 Multiple TouchStar Devices

Connection:

If multiple devices are to be connected to the modem, there are 2 parts of the connection. The first part is to connect the modem to the interface converter; the second part is to connect the interface converter to the first TouchStar device. If you notice, the second part is actually exactly similar to the connection described in “**Chapter 6.2 - Using RS-422 and RS-485 (page 80)**”. As such, we would only look at the connection for the first part. Both 25-pin and 9-pin modems would be looked at.

a) 25-pin Modem

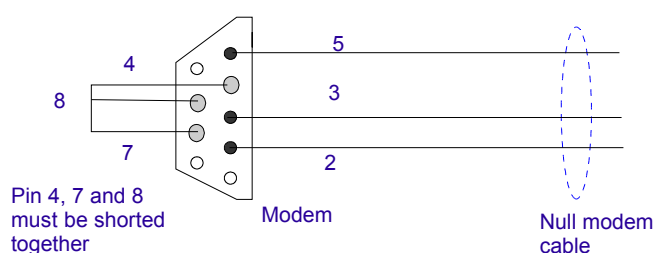


Pin-out:

Modem	Interface Converter
2	Rx
3	Tx
7	Ground

Connecting a 25-pin modem to the interface converter

b) 9-pin Modem



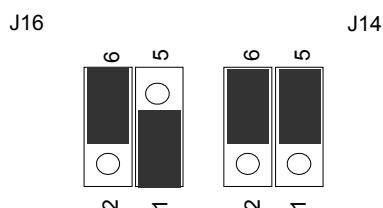
Pin-out:

Modem	Interface Converter
3	Rx
2	Tx
5	Ground

Connecting a 9-pin modem to the interface converter

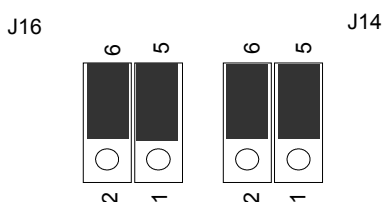
Jumpers:

For RS-422, the jumpers of all devices should be connected as shown:



Jumper Settings for RS-422

For RS-485, the jumpers of all devices should be connected as shown:



Jumper Settings for RS-485

Menu Setting:

You would need to configure the Device IDs of the individual devices uniquely. The Baud Rate of all devices should also be similar.

However, please note that you should only configure the first device in the network to the Modem type, while the rest of the devices are to be configured to either the RS-422 type or the RS-485 type (depending on which is used). This is because only one device can handshake with the modem.

Follow the menu setting described in "**Chapter 4.2.5d - Setting the Communication Type (page 42)**".

Notes:

Configure the first device with the Modem type. Configure the rest of the other devices to the RS-422 or RS-485 type (depending on which is the one that is used).

Application Program Setting:

The Device IDs you choose under the respective menus described above should be the same as that configured in the application program.

Chapter 7

7 Setting Up for Access Control

Access control can be effected in one of the following ways:

- 1) Using a third party controller
- 2) Using the TouchStar Door Zone Controller (or known as DZC)

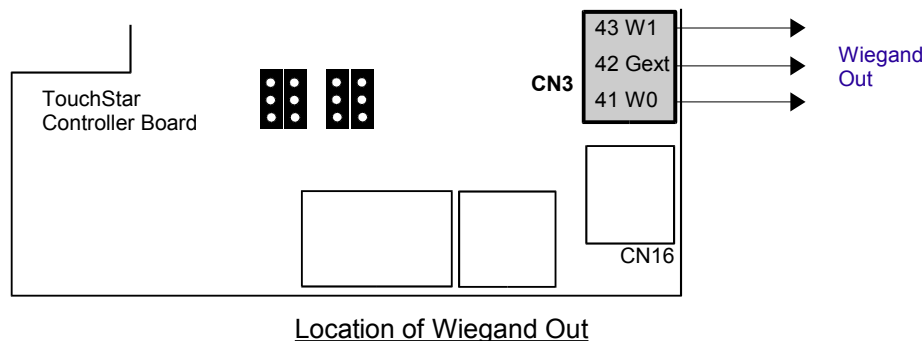
Let's look at how these can be done.

7.1 Using a Third Party Door Controller

When the Wiegand output setting is enabled at the device, TouchStar would generate and send the Wiegand data (ID with site code and system code) to the external controller upon a successful authentication. For the Wiegand data to be recognizable, the external controller must also use the same Wiegand format. Let us look at the connection and menu settings that are required.

Connection:

Connect W0, W1 and Gext (External Ground) of CN3 to the Wiegand input of the third party controller.



Menu Setting:

Under the WIEGAND menu (see "**Chapter 4.2.5f - Configuring the Wiegand Settings (page 48)**"):

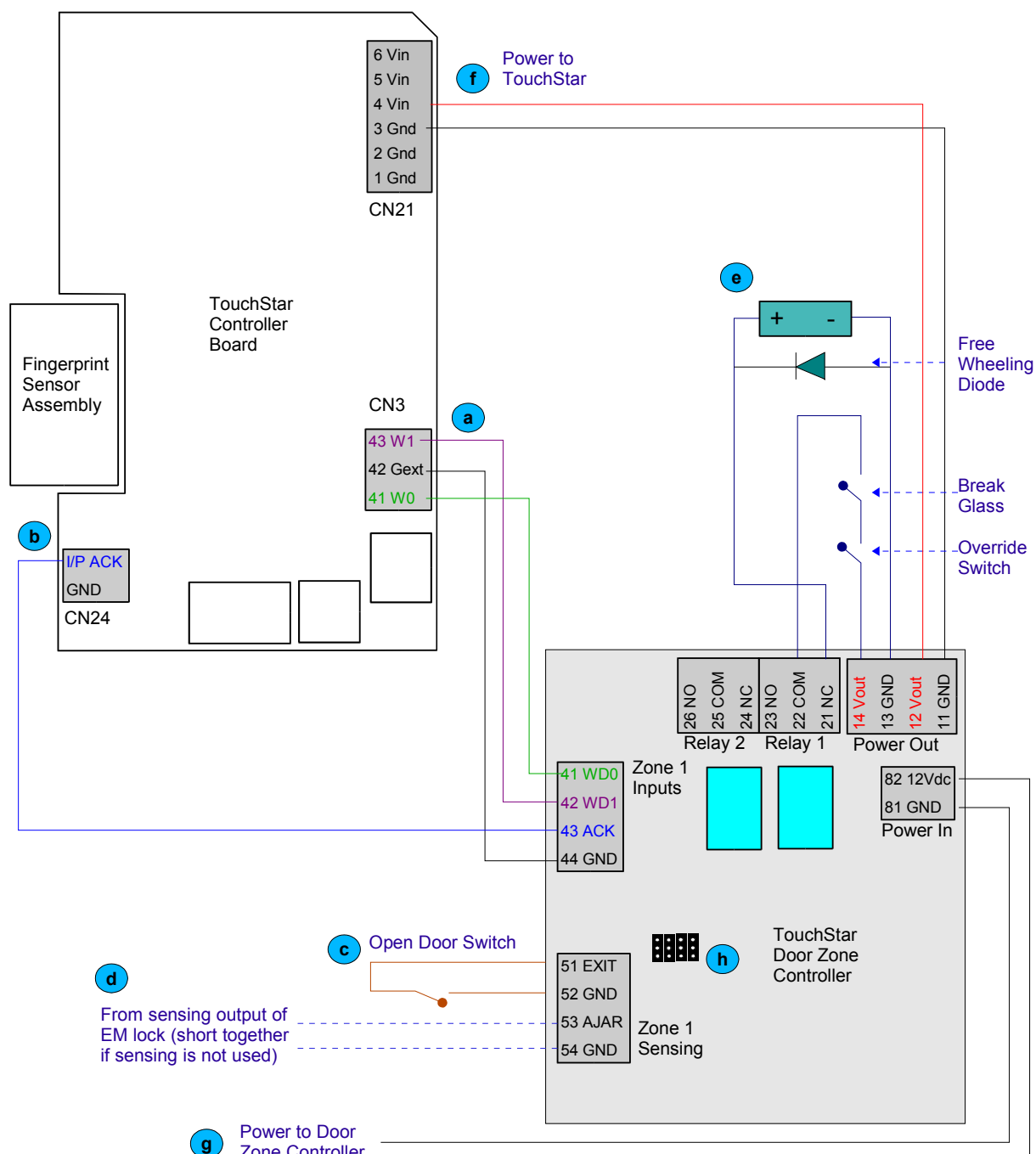
- a) Set FORMAT to the desired Wiegand format.
- b) Set WIEGAND OUT to ENABLE.
- c) Configure the default SITE CODE that would be used.

CONFIG WIEGAND	
FORMAT	:26 BITS V1
WIEGAND OUT	:ENABLE
SITE CODE	:001
SEL	EXIT
ENTER	

7.2 Using the TouchStar Door Zone Controller

The TouchStar Door Zone Controller (DZC) can be used as a source of power to both the TouchStar device and the electromagnetic lock. The connection and settings are described as follows:

Connection:



Using the TouchStar Door Zone Controller

- a) Connect W0, W1 and Gext (external ground) of CN3 in TouchStar to the DZC (pin 41, 42 and 44 respectively).
- b) Connect the Wiegand Acknowledge of CN24 in TouchStar to ACK of DZC (pin 43).
- c) Connect the open door switch (pin 51 and 52 of DZC).
- d) If door sensing is used, connect pin 53 and 54 of DZC to the sensing outputs of the door sensor. If sensing is not used, these 2 points should be shorted together.
- e) Connect the EM lock as shown. Please note that pin 14 and 22 of DZC must be connected in order to complete the electrical path. The break glass and override switch can be connected as shown.
- f) Connect cable as shown to allow the DZC (pin 11 and 12) to supply power to TouchStar later.
- g) Connect cable as shown so that the DZC (pin 81 and 82) can be powered up later.
- h) Configure the jumpers to set the relay open duration for the door (see "**Appendix C – TouchStar Door Zone Controller (page 95)**").

Menu Setting:

- 1) Under the WIEGAND menu (see "**Chapter 4.2.5f - Configuring the Wiegand Settings (page 48)**"):
 - a) Set WIEGAND OUT to TS CONT.
 - b) The FORMAT setting does not matter.

CONFIG WIEGAND			
FORMAT	:	26 BITS V1	
WIEGAND OUT	:	TS CONT	
SEL	EXIT		ENTER

- 2) Under the DOOR menu (see "**Chapter 4.2.5c - Setting the Door Control (page 41)**"):
 - a) Set LOCK DOOR to DISABLE.

CONFIG DOOR			
SETTING	:	DEFAULT	
LOCK DOOR	:	DISABLE	
SEL	EXIT		ENTER

Summary for this Chapter

This chapter has described how you can make use of door controllers for access control. The TouchStar controller board actually has an on-board relay that can be used to control the electromagnetic lock. However, this method of controlling is not as secure as if an external door controller were to be used. Nevertheless, if you are interested in a simple door control solution using the on-board relay, you can refer to "**Appendix D – Using the On-board Relay for Door Control (page 97)**".

Chapter 8

8 Appendices

Appendix A – Technical Specifications

Supply Voltage	12 to 24 VDC
Power Consumption	< 5 W
Operating Environment [for indoor use only]	Ambient temperature 0°C ~ 60°C Humidity 10 ~ 90% RH
Dimension	158 x 240 x 73 mm
Weight	< 1 kg
Fingerprint Storage	720 fingerprint templates [basic] [optional 4400 fingerprint templates]
Event Log	At least 20,000 records [store in non-volatile memory]
Comm Interface	RS-232 / RS-485 / RS-422 / Wiegand [multi-format]
Micro-controller	32-bit 96 MHz
Memory	Flash 32 MBit
LCD	128 x 64 graphic with LED backlight
LED	2 [pass / fail]
Clock / Calendar	Battery backup
Keypad	16 keys [with 4 Function keys]
Input	1
Relay	1 [for bell control]
Material	- Keypad [silicon rubber] - Enclosure [high impact PC-ABS]
Built-in	Contactless card reader [HID Standard / Keri / Mifare / EM]
Optional	- Smart card interface - Barcode reader [external] - Magnetic stripe reader [external] - Modem [external] - Ethernet [built-in] - Stainless steel flush mount modem available - Door Zone Controller / Relay Control Board [external]
Fingerprint Sensor Type	Optical
Fingerprint Sensor Resolution	500 dpi
Effective Sensing Area	13.1 [W] x 15.1 [L] mm
Minutiae Size	400 bytes [encrypted]

Appendix B – TCP/IP Subnet Mask Translation

An IP address is made of the **network section** and the **host section**.

A netmask defines how many bits from the IP address are to be taken as the network section and how many bits are to be taken as the host section.

The Subnet Mask setting in TouchStar follows the number of host bits.

Hence, for example, if the subnet mask in your network is 255.255.255.0, you should use 8 as the Subnet Mask setting. The following table shows all the possible translations for the Netmask to the number of host bits.

Subnet Mask Translation Table

Netmask	Subnet Mask Setting or No. of Host Bits
255.255.255.252	2
255.255.255.248	3
255.255.255.240	4
255.255.255.224	5
255.255.255.192	6
255.255.255.128	7
255.255.255.0	8
255.255.254.0	9
255.255.252.0	10
255.255.248.0	11
255.255.240.0	12
255.255.224.0	13
255.255.192.0	14
255.255.128.0	15
255.255.0.0	16
255.254.0.0	17
255.252.0.0	18
255.248.0.0	19
255.240.0.0	20
255.224.0.0	21
255.192.0.0	22
255.128.0.0	23
255.0.0.0	24

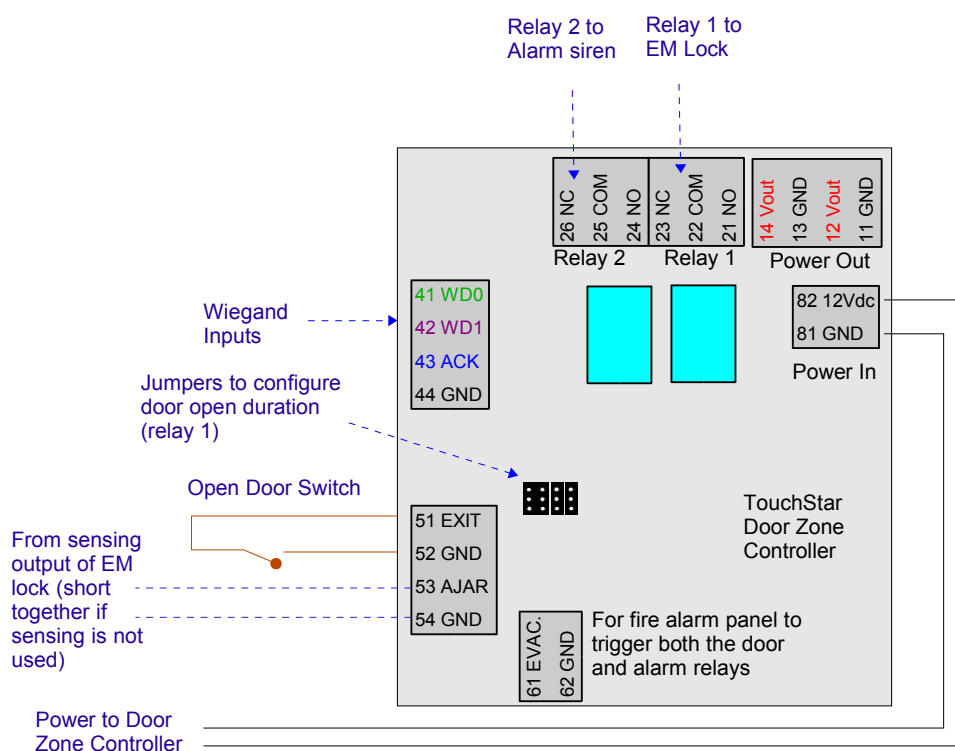
Appendix C – TouchStar Door Zone Controller

This appendix briefly describes how the TouchStar Door Zone Controller (DZC) works. For more detailed instructions and precautions to be taken, you may refer to “**TouchStar Door Zone Controller User's Manual**”.

How DZC works:

The TouchStar DZC is a standalone controller that interfaces directly to TouchStar to provide door control function. It is capable of monitoring, securing and opening the door upon detecting the exit request through Wiegand signaling. Alarm would be triggered upon detecting system intrusion or system fault.

Each door zone controller can currently control one door. The control is managed using two dry contact relays. One of the relays is used to control the door through the EM lock (or other electromechanical door) while the other relay is used to trigger an alarm signal when the alarm condition is met.



Schematic Layout of DZC

DZC can be jumper-configured for the door open duration. A row of four jumpers control the door open duration as tabulated below :

Jumpers to configure Door Open Duration:

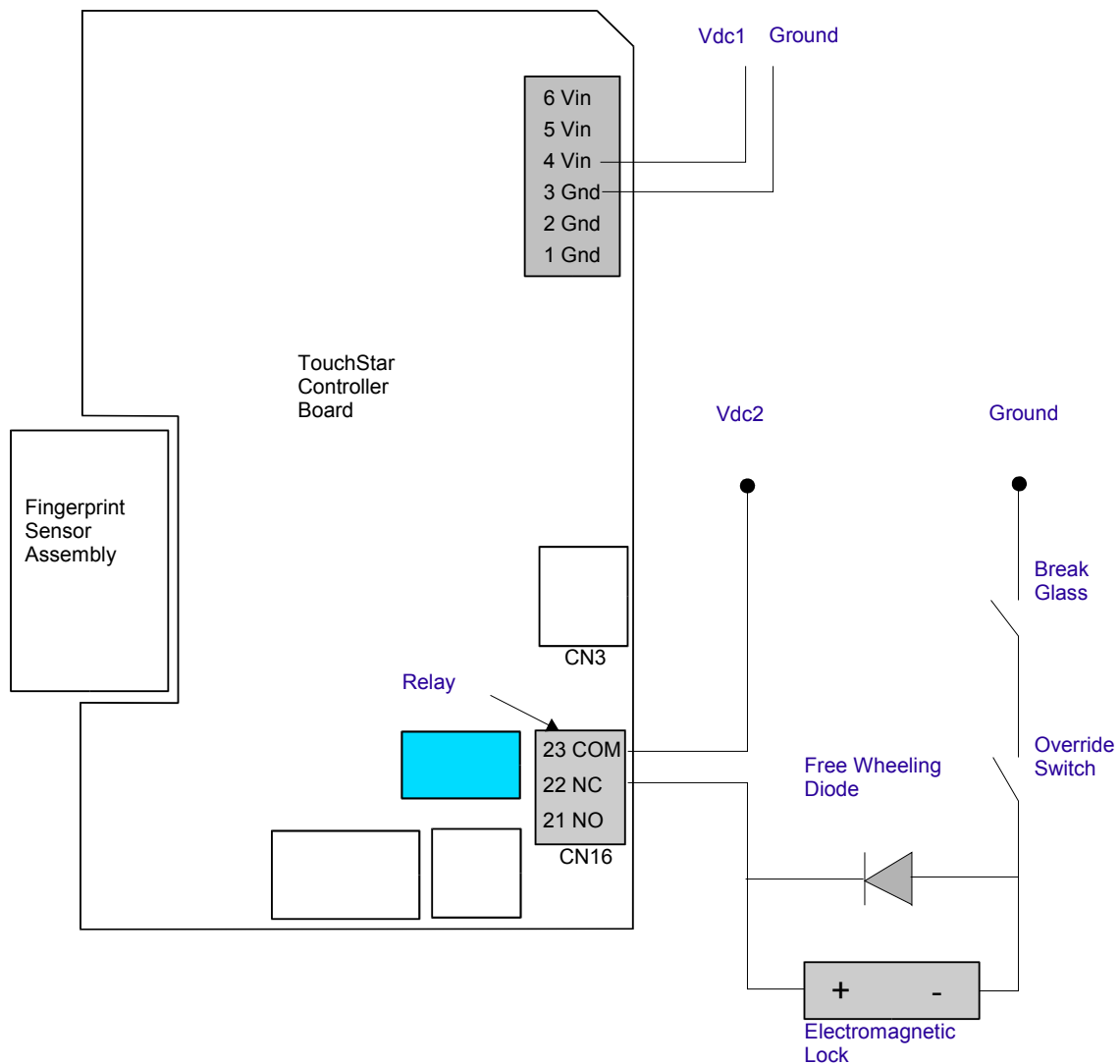
J5			J6			J7			J8			Open door duration (seconds)
1	2	3	1	2	3	1	2	3	1	2	3	
												0
												5
												10
												15
												20
												25
												30
												35
												40
												45
												50
												55
												60
												65
												70
												75

Appendix D – Using the On-board Relay for Door Control

This method of controlling the door is actually not recommended because it is not as secure as using an external door controller. For knowledge and completeness, the connection is still presented here in case you are interested.

Connection:

a) The electromagnetic lock is connected directly to CN16 as shown.



Using the relay to control the door

Menu Setting:

- 1) Under the WIEGAND menu (see "**Chapter 4.2.5f - Configuring the Wiegand Settings (page 48)**"):
 - a) Set WIEGAND OUT to DISABLE.
 - b) The FORMAT setting does not matter.

CONFIG WIEGAND			
FORMAT :26 BITS V1			
WIEGAND OUT :TS CONT			
SEL	EXIT		ENTER

- 2) Under the DOOR menu (see "**Chapter 4.2.5c - Setting the Door Control (page 41)**"):
 - a) Set LOCK DOOR to DISABLE.

CONFIG DOOR			
SETTING :[DEFAULT]			
LOCK DOOR :DISABLE			
SEL	EXIT		ENTER

- 3) Under the RELAY menu (see "**Chapter 5.1.2e - Configuring the Relay Option (page 61)**"):
 - a) Set the RELAY TYPE to ENABLE.

SET RELAY TYPE			
SELECT → ENABLE			
SEL	EXIT		ENTER

- b) Next, set the DURATION. This is the duration that the door would open before it would close again.

CONFIG RELAY			
SETTING :[DEFAULT]			
DURATION(SECS) :05			
SEL	EXIT		ENTER

Appendix E – ADAM 4520 RS-232 to RS-422 / 485 Interface Converter

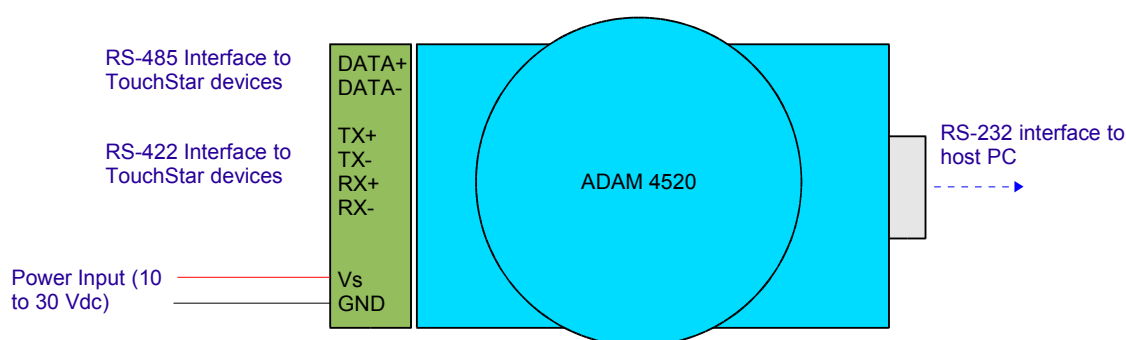
Several interface converters are available in the market, however, one that has been tested to be working with the TouchStar devices is the ADAM 4520 unit.

In this appendix, the connections and pin-outs of the ADAM 4520 unit are presented. You can also find the same information in the manuals that come with the acquisition of the unit.



Powering the unit:

Power the converter unit with any unregulated power source between +10 and +30 Vdc.



ADAM 4520 Interface Converter

RS232 Cable Connection:

The table below shows the pin to pin connection between the RS-232 port of the ADAM Converter module and the COM port of the host PC.

Pin-out:

	ADAM 4520 (D-SUB 9-pin male connector)	PC (COM Port) (D-SUB 9-pin female connector)
Tx	2	2
Rx	3	3
GND	5	5

Switches and Jumper Settings:

The following tables illustrate the possible switch settings for the ADAM Converter when you open up the module.

You would find that in the converter board, there are 2 switch settings. One of it is labeled as SW1 while the other is labeled as SW2. SW1 controls the data format settings.

TouchStar uses the 10 bits data format (8 data bits, no parity, 1 stop bit and 1 start bit). Hence, you will need to set SW1 to the 10 bits data format (Table 1).

Table 1:

ADAM 4520 Data Format Settings (SW1)		
Data Format	1	2
9 bits	-	-
10 bits	ON	-
11 bits	-	ON
12 bits	ON	ON

SW2 controls the baud rate settings and the communication mode used (whether RS422 and RS485).

If you are using RS422, you need only to turn on the **RS-422** switch (**Sw 10**), leaving the rest of the switches at the **OFF** position.

If you are using RS485 however, turn off the **RS-422** switch (**Sw 10**), and turn on the switch for the desired baud rate. Take note the baud rate you set on the module must be the same as that configured at the device and that used at the application program.

Table 2:

ADAM 4520 Baud Rate Settings (SW2) for											
Baud Rate	Sw	1	2	3	4	5	6	7	8	9	10
RTS control	1	ON	-	-	-	-	-	-	-	-	-
1200 bps	2	-	ON	-	-	-	-	-	-	-	-
2400 bps	3	-	-	ON	-	-	-	-	-	-	-
4800 bps	4	-	-	-	ON	-	-	-	-	-	-
9600 bps	5	-	-	-	-	ON	-	-	-	-	-
19.2 Kbps	6	-	-	-	-	-	ON	-	-	-	-
38.4 Kbps	7	-	-	-	-	-	-	ON	-	-	-
57.6 Kbps	8	-	-	-	-	-	-	-	ON	-	-
115.2 Kbps	9	-	-	-	-	-	-	-	-	ON	-
RS-422	10	-	-	-	-	-	-	-	-	-	ON

Legend

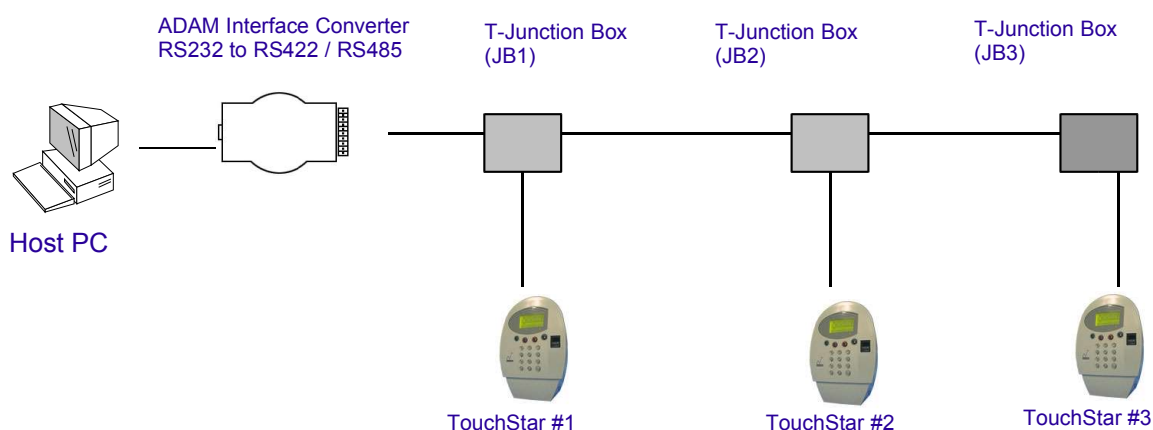
- = OFF

Appendix F – Using the ADAM-4520 in RS-422 and RS-485 Communication

The following examples show how three TouchStar Mini devices are connected in daisy chain using RS422 first and RS485 next. The connection makes use of T-Junction boxes (JB-422). Please consult your dealer for the acquisition of the junction boxes.

The following diagram shows a schematic layout of the connection. Appendix E can be referred to for a pin-out description for the RS-422 or RS-485 signals at the ADAM. ADAM configurations are also described in Appendix E.

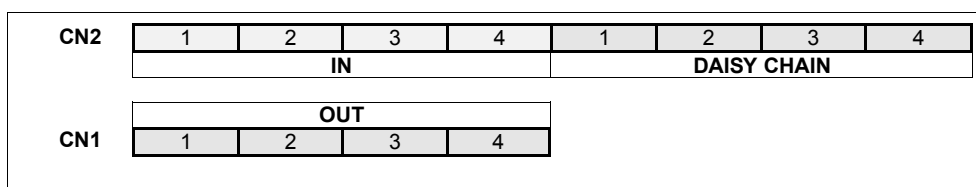
Note that the placement of terminating resistors at the ADAM and at the last T-Junction box depends on actual testing. For the TouchStar devices communicating in RS-485, terminating resistors are usually not needed. This has been tested by the manufacturer.



TouchStar devices in RS422 or RS485

T-Junction Box:

The diagram below shows a schematic layout of the T-Junction box. There are three main sections for the pin-outs, namely 'IN', 'OUT' and 'DAISY CHAIN'. Each pin number of a section is internally shorted to the similar pin number of the other two sections.

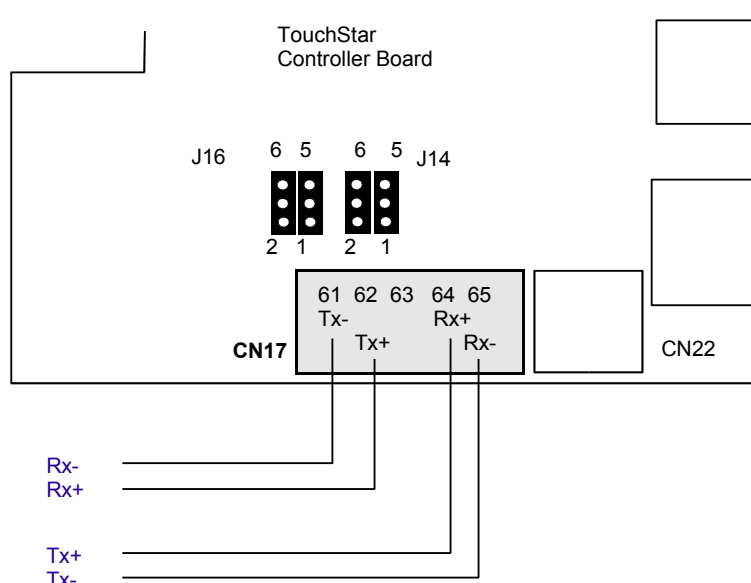


Layout of T-Junction Box

If this is the first T-Junction box from the ADAM, the RS-422 or RS-485 signals go into the 'IN' section. The signals from the 'OUT' section go into the TouchStar unit. And the signals from the 'DAISY CHAIN' section go into the next T-Junction box.

The recommended colors of the wires to use are also shown in the diagrams that follows.

RS-422 Connection



Pin-out:

ADAM	TouchStar (CN17)
Rx-	61 (Tx-)
Rx+	62 (Tx+)
Tx-	64 (Rx+)
Tx+	65 (Rx-)

RS-422 cable pin-out from ADAM to TouchStar

1) Connection between ADAM and JB1

ADAM	Color of Wire*	JB1 (Pin No. at 'IN')	Remarks
Tx+	Blue	1	120 Ohms terminating resistor across Tx+ and Tx- at ADAM's end if necessary
Tx-	Blue/White	2	
Rx+	Orange	3	120 Ohms terminating resistor across Rx+ and Rx- at ADAM's end if necessary
Rx-	Orange/White	4	

*Any wires in the RS422 cable can be used. The color scheme used is shown only as a guide.

2) Connection between JB1 and JB2

JB1 (Pin No. at 'DAISY CHAIN')	JB2 (Pin No. at 'IN')	Remarks
1	1	-
2	2	-
3	3	-
4	4	-

3) Connection between JB and TouchStar

JB (Pin No. at 'OUT')	TouchStar		
	Pin No.	Representation	Color of Wire Connected at Pin**
1	64	Rx+	Blue
2	65	Rx-	Blue / White
3	62	Tx+	Orange
4	61	Tx-	Orange / White

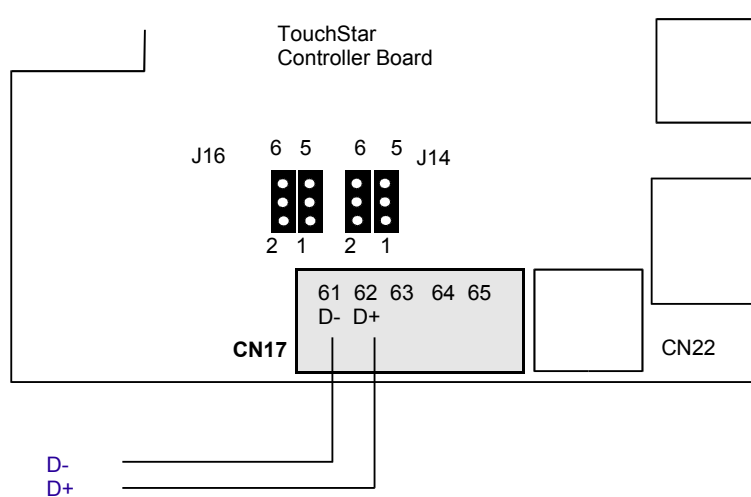
** This color scheme used is consistent with that shown in (1).

4) Connection at JB3 (last junction box or end of line)

JB3 (Pin No. at 'OUT')	Remarks
1	120 Ohms terminating resistor across Pin nos. 1 and 2 if necessary
2	
3	120 Ohms terminating resistor across Pin nos. 3 and 4 if necessary
4	

At each T-Junction box, the drain wires of the interconnecting branches must be shorted together.

RS-485 Connection



Pin-out:

ADAM	TouchStar (CN17)
D-	61 (D-)
D+	62 (D+)

RS-485 cable pin-out from ADAM to TouchStar

1) Connection between ADAM and JB1

ADAM	Color of Wire*	JB1 (Pin No. at 'IN')	Remarks
D+	Blue	1	Terminating resistors should not be necessary
D-	Orange	2	

*Any wires in the RS485 cable can be used. The color scheme used is shown only as a guide.

2) Connection between JB1 and JB2

JB1 (Pin No. at 'DAISY CHAIN')	JB2 (Pin No. at 'IN')	Remarks
1	1	-
2	2	-

3) Connection between JB and TouchStar

JB (Pin No. at 'OUT')	TouchStar		
	Pin No.	Representation	Color of Wire Connected at Pin**
1	6	D+	Blue
2	7	D-	Orange

** This color scheme used is consistent with that shown in (1).

4) Connection at JB3 (last junction box or end of line)

JB3 (Pin No. at 'OUT')	Remarks
1	Terminating resistors should not be necessary
2	

At each T-Junction box, the drain wires of the interconnecting branches must be shorted together.

Appendix G – Testing or Troubleshooting TCP/IP Connections

Network problems are constantly a source of hiccups during system installation. This appendix describes some basic troubleshooting steps for TouchStar devices fitted with the Ethernet add-on board (ECom) for TCP/IP communication.

The problem commonly faced is tabulated below:

	Error reported at Application Program	Description	What to check
	Error code 163 (A3 hex) - Connection Fail	Unable to connect to IP address and/or TCP Port specified in the application program.	Follow the troubleshooting steps below.

Step 1 : Check whether host PC can ping to TouchStar

- 1) In MS-DOS, perform a **Ping** command to the specified IP address.

```
C:\>ping 90.0.0.61
```

- 2) Check whether there is any response. A typical response will look as follows:

```
Pinging 90.0.0.61 with 32 bytes of data
```

```
Reply from 90.0.0.61: bytes=32 time<10ms TTL=32
Reply from 90.0.0.61: bytes=32 time<10ms TTL=32
Reply from 90.0.0.61: bytes=32 time<10ms TTL=32
Reply from 90.0.0.61: bytes=32 time<10ms TTL=32
```

If there is a response, proceed to Step 2.

If there is no response, it means that the Ethernet add-on card (ECom) cannot be located in the network. Please verify that the IP Address configured on ECom is correct, or check with your network administrator.

Step 2 : Check whether host PC can Telnet to TouchStar

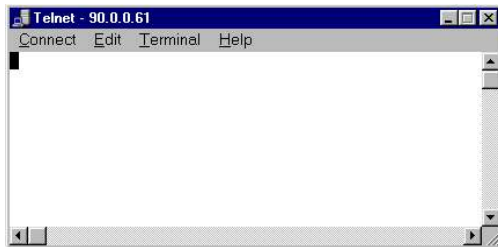
- 1) Execute the following **Telnet** command. The telnet command will connect to the particular TCP Port number that was specified during the configuration of the TCP/IP parameters.

If the TCP Port number is 4567, the command will be:

```
C:\>telnet 90.0.0.61 4567
```

2) Check whether there is any response.

If the telnet command is successful, a new window with the IP address specified in its header will appear as shown below. Try the Poll Device command in the host software next.



If the telnet is not successful, check that the IP Address that you used to ping correctly belongs to TouchStar. You can verify this by doing an **ARP** command. This command will obtain the Physical Address of the network device being pinged.

```
C:\>arp -a
```

The result of the ARP command will typically be:

```
Interface: 90.0.0.61
Internet address      Physical Address      Type
90.0.0.61             00:0A:60:00:01:12     Dynamic
```

The physical address of ECom is printed on a label on board. Verify this with the above output.

If the physical addresses are different, this explains why the telnet command was not successful, but the ping command was. The response to ping was not from ECom. It was from any device (may be another PC) configured with the same IP address.

If the physical addresses are the same, check the TCP Port setting on ECom to ensure it is the same port number that the Telnet command used.

Appendix H – Log Types in TouchStar

The TouchStar device handles 4 types of log records listed as follows :

- Transaction Log**
 A transaction log is recorded upon a successful authentication. Each log contains the User ID of the user performing the authentication, as well as the date and time.
- Fail Attempt Log**
 A fail attempt log is recorded when the authentication process fails.
- Trace Event Log**
 A trace event log is recorded whenever any critical event has occurred during local administration or during operation (such as when the device was being tampered with).
- Authentication Mode Trace**
 An authentication mode trace log is recorded after the transaction log has been recorded. It records which authentication property was used to achieve the successful authentication. This log also indicates whether the ID was entered using the keypad, or was captured from a card scan.

Each log record carries with it a type value to indicate what log it is. The following tables show the various types of logs and the circumstances under which they would be recorded.

Table 1: Transaction Log

The type of time attendance log recorded depends on the field-descriptor set that is chosen, and the selected field when the user performs his authentication.

Log Type	Field Descriptor Set						
	(a) Welcome	(b) Attd/Access	(c) Attd/Access V1	(d) Attd (2 Levels)	(e) Attd (6 Levels)	(f) Attd (7 Levels)	(g) Attd/Access V2
1	Welcome	Attendance		In	Attendance-In	Waktu Masuk	In
2		Access Control	Access Control	Out	Leaving-Out	Waktu Keluar	Out
3					Early Leave	Hujan	Access Control
4					Going Out	Hospital	
5					Return	Jalan Sesak	
6					Others	Kndrn Rosak	
7			In			Anak Sakit/Skl	
8			Out				

Table 2: Trace Event Log

	Log Type	Event	Additional Description
Event related to the alarm indication			
1	28 (1C hex)	Tamper switch opened	See note 1
2	29 (1D hex)	Tamper switch closed	See note 1
3	48 (30 hex)	Alarm activated	Recorded if there was an alarm event from TouchStar Door Zone Controller (DZC). See note 1
4	49 (31 hex)	Alarm deactivated	Recorded if the alarm event from TouchStar DZC was subsequently disabled. See note 1.
5	129 (81 hex)	Activated alarm was acknowledged and disabled	The tamper switch being opened will cause the alarm indication via the 1 st LED to be shown. If TDM subsequently sends a command to TouchStar to disable the alarm indication, this log will be recorded.
Events related to the device powering up			
6	144 (90 hex)	Device powered up	Recorded when the TouchStar powers up.
7	145 (91 hex)	Start-up error	Recorded when there are errors during power up.
Events related to the administration modes			
8	160 (A0 hex)	Administration mode was entered	-
9	161 (A1 hex)	Administration mode was exited	-
10	178 (B2 hex)	A user was added	Recorded when a user is added, be it using fingerprint, card only or card with PIN. If the user uses fingerprint, and enrolls three fingerprints for the same User ID, there will be three such consecutive logs.
11	179 (B3 hex)	A user was deleted	-
12	180 (B4 hex)	A master was added	-
13	181 (B5 hex)	A master was deleted	-
Events related to door configuration			
14	209 (D1 hex)	Door secure	Recorded when the <i>DoorLockUnlock</i> setting is configured as " <i>Always Locked</i> ".
15	210 (D2 hex)	Door unsecure	Recorded when the above setting is configured as " <i>Always Unlocked</i> ".
16	211 (D3 hex)	Door normal	Recorded when the above setting is configured as " <i>Disable</i> " or " <i>By Schedule</i> ".

Note 1 : The **Alarm** setting must be enabled for this log to be recorded.

Table 3: Fail Attempt Logs

	Log Type	Event	Description
<i>Events related to authentication</i>			
1	231 (E7 hex)	Fail fingerprint matching	-
2	232 (E8 hex)	Fail card matching	-
3	233 (E9 hex)	Fail card with PIN matching	-
4	234 (EA hex)	ID was not found	-
5	235 (EB hex)	Fingerprint match was not found using Speed Search	-
6	236 (EC hex)	Matching was aborted	-
7	243 (F3 hex)	Access denied due to being out of defined schedule	See note 2
8	244 (F4 hex)	Access denied due to time-zone information downloaded to the device was insufficient	See note 2
9	246 (F6 hex)	Access denied due to authentication profile error	See note 2
<i>Events related to Wiegand Acknowledge</i>			
10	245 (F5 hex)	Wiegand acknowledge was not received	-
<i>Events related to authentication without using the card for providing ID input</i>			
11	247 (F7 hex)	Card input required for card with fingerprint authentication	-
12	248 (F8 hex)	Card input required for card with PIN authentication	-
13	249 (F9 hex)	Card input required for card only authentication	-
14	250 (FA hex)	One to many matching – user found was enrolled with card with fingerprint	-
15	251 (FB hex)	Partial user matching – user found was enrolled with card with fingerprint	-

Note 2: This log will be recorded when timezone checking is enabled.

Table 4: Authentication Mode Trace

	Log Type	Event	Description
1	213 (D5 hex)	Card input was used to provide the ID while authenticating a fingerprint record enrolled with ID captured from card scan.	-
2	214 (D6 hex)	Keypad input was used to provide the ID while authenticating a fingerprint record enrolled with ID captured from card scan.	-
3	215 (D7 hex)	Card input was used to provide the ID while authenticating a fingerprint record enrolled with ID entered from the keypad.	-
4	216 (D8 hex)	Keypad input was used to provide the ID while authenticating a fingerprint record enrolled with ID entered from the keypad.	-
5	217 (D9 hex)	Card input was used to provide the ID while authenticating a PIN record enrolled with ID captured from card scan.	-
6	218 (DA hex)	Keypad input was used to provide the ID while authenticating a PIN record enrolled with ID captured from card scan.	-
7	219 (DB hex)	Card input was used to provide the ID while authenticating a PIN record enrolled with ID entered from the keypad.	-
8	220 (DC hex)	Keypad input was used to provide the ID while authenticating a PIN record enrolled with ID entered from the keypad.	-
9	221 (DD hex)	Card only authentication was carried out.	-
10	222 (DE hex)	Speed Search was used to authenticate a record enrolled with ID captured from a card scan.	-
11	223 (DF hex)	Speed Search was used to authenticate a record enrolled with ID entered from the keypad.	-
12	224 (E0 hex)	One-to-many matching was used to authenticate a record enrolled with ID captured from a card scan	-
13	225 (E1 hex)	One-to-many matching was used to authenticate a record enrolled with ID entered from the keypad.	-

Appendix I – Care and Maintenance

TouchStar is a very rugged device which can operate trouble-free for many years. Although no stringent maintenance and handling requirement is required, some basic caring, and precaution is still needed to ensure good and reliable performance.

Cleaning and caring:

Never use a sharp object to scrape deposits from the fingerprint sensor. Permanent damage will result.

The fingerprint sensor normally do not require routine cleaning if there is no noticeable degradation of fingerprint verification performance. However, for general cleaning, wipe the fingerprint sensor with a piece of dry and soft tissue paper.

Only use 99% pure Isopropyl Alcohol and lightly damp a piece of soft foam, soft cotton cloth or soft tissue paper to remove oily deposits or dirt from the fingerprint sensor or the enclosure surface.

Do not use wet (soiled or excessive moisture) cloth to clean the sensor or its surrounding because the liquid can diffuse into the enclosure or the fingerprint sensor.

When cleaning the fingerprint sensor or the enclosure surface, it is normally not required to switch off the power supply

After cleaning the fingerprint sensor, always allow two minutes for the liquid to dry up (before resume using it).

Preventive maintenance:

The fingerprint sensor and other electronics devices inside the TouchStar device do not require routine calibration or preventive maintenance.

The optical based fingerprint sensor can withstand harsh environment and ESD; nevertheless, adequate precaution has to be taken to prevent degradation. Do not expose the device to intense sunlight, operate or storage environment exceeding the rated specification. Fingerprint sensor should not be exposed to excessive moisture or condensation.

Ensure wiring is secured to the screw terminal blocks and the screw terminal blocks are fully inserted.

Inspection maintenance frequency:

Conduct weekly inspection to check for damages on the LCD display, key buttons or enclosure. As mentioned, it is normally not required to conduct routine cleaning of fingerprint sensor if there is no noticeable degradation of fingerprint verification performance.