



Technical User Manual GHTER-XX



**Technische gebruikers handleiding
Gezichtherkenning Terminal**

GHTER-XX

Inhoudsopgave

| | | |
|--------|--|----|
| 1 | Welcome | 2 |
| 2 | Hardware Installation | 3 |
| 2.1 | Item Checklist | 3 |
| 2.2 | Size and Weight Specifications | 3 |
| 2.3 | Voor- en zij aanzicht met maatvoering | 4 |
| 2.4 | Maatvoering montageplaat | 4 |
| 2.5 | GHTER-XX Port Pins and Switches | 5 |
| 2.6 | DIP Switch | 6 |
| 2.7 | Reset Button | 7 |
| 2.8 | Terminal Block Port Pins | 7 |
| 2.8.1 | • P1: Power Supply Port | 8 |
| 2.8.2 | • P2: Digital I/O Port | 8 |
| 2.8.3 | • P3: Communication Port | 8 |
| 2.9 | Wiring Schematic | 9 |
| 2.10 | Typical Wiring Schematics | 9 |
| 2.11 | Turning On and Status Lights | 11 |
| 2.12 | Networking with Computer | 11 |
| 3 | Software Setup | 12 |
| 3.1 | Accessing GHTER-XX through Web Interface | 12 |
| 3.2 | Basic Features | 13 |
| 3.3 | Status | 13 |
| 3.4 | Log | 14 |
| 3.5 | User Management | 17 |
| 3.6 | Schedule | 20 |
| 3.7 | Advanced Features | 21 |
| 3.8 | Facial Recognition | 21 |
| 3.9 | Network | 22 |
| 3.10 | I/O Control | 23 |
| 3.11 | Wiegand | 24 |
| 3.11.1 | Defining Custom Format for Wiegand Input Interface | 25 |
| 3.12 | Display | 27 |
| 3.13 | Log Configuration | 27 |
| 3.14 | Time | 28 |
| 3.15 | Password | 29 |
| 3.15.1 | Admin Username and Password | 29 |
| 3.15.2 | User Username and Password | 29 |
| 3.15.3 | Passcode | 29 |
| 3.15.4 | System | 29 |
| 3.15.5 | Power Saving Time | 30 |
| 3.15.6 | Motion Detector Sensitivity | 30 |
| 3.15.7 | Display Language | 30 |
| 3.16 | Firmware | 31 |

| | | |
|-------|---|----|
| 4 | Standalone Mode | 32 |
| 4.1 | How to Use a Keypad in Standalone Mode..... | 32 |
| 4.2 | Operations in Standalone Mode | 32 |
| 4.3 | Enter standalone mode for the very first time | 33 |
| 4.4 | How to enroll | 33 |
| 4.5 | Enter Standalone Mode after the first root user enrollment..... | 34 |
| 4.6 | Menus of Standalone Mode | 34 |
| 4.7 | Status..... | 34 |
| 4.8 | Log | 35 |
| 4.9 | User | 35 |
| 4.10 | Setup | 36 |
| 5 | Facial Enrollment and Recognition..... | 38 |
| 5.1 | Enrollment | 38 |
| 5.2 | Recognition | 41 |
| 6 | Troubleshooting..... | 43 |
| 6.1.1 | • How do I keep my firmware up to date?..... | 44 |
| 6.1.2 | • Where can I find my GHTER-XX product serial number? | 44 |
| 6.1.3 | • What about service and support?..... | 44 |
| 7 | Last But Not Least..... | 45 |
| 7.1 | Safety in Using and Handling GHTER-XX..... | 45 |
| 7.2 | FCC Regulatory Compliance Information | 45 |
| 8 | Appendix | 47 |
| 8.1 | Product Specifications..... | 47 |
| 8.2 | Acronym List..... | 48 |
| 8.3 | Factory Default Configuration Settings..... | 49 |

I Welcome

Congratulations on purchasing an GHTER-XX system! Equipped with state-of-the-art Near Infrared Facial Recognition and DSP technology, your GHTER-XX Embedded Facial Recognition System provides the accuracy and speed required by mission-critical as well as commercial applications. GHTER-XX is designed for easy installation, integration, and operation. To quickly learn how to setup and operate your GHTER-XX as a standalone system, please refer to the Quick Start Guide.

If you wish for a complete experience of your GHTER-XX, please continue with this user manual. This manual covers GHTER-XX hardware setup, software management, user operation, system troubleshooting and safety information.

Let's start your GHTER-XX experience!

Important Notes

- 1. For your safety, please pay special attention to the safety information in Chapter 7**

2 Hardware Installation

This chapter guides you through GHTER-XX hardware installation procedure and discusses the following topics:

- Item check list
- Size and weight specifications
- GHTER-XX Terminal port pins and switches
- GHTER-XX Terminal wiring schematics

2.1 Item Checklist

The following items are included in the GHTER-XX package.

- ✓ GHTER-XX Terminal (Refer as GHTER-XX)
- ✓ Mounting Bracket
- ✓ Quick Start Guide
- ✓ Product CD-ROM

2.2 Size and Weight Specifications

Table 2-1 shows the size and weight specifications of your GHTER-XX Terminal. Figure 2-1 and 2-2 show the dimensions of the GHTER-XX Terminal and the mounting bracket.

For smooth installation, it is suggested to use the mounting bracket to mount the GHTER-XX Terminal on a wall.

| | GHTER-XX |
|-----------|----------|
| Length | 175 mm |
| Width | 88 mm |
| Thickness | 80 mm |
| Weight | 800 gram |

Table 2-1

2.3 Voor- en zijaanzicht met maatvoering

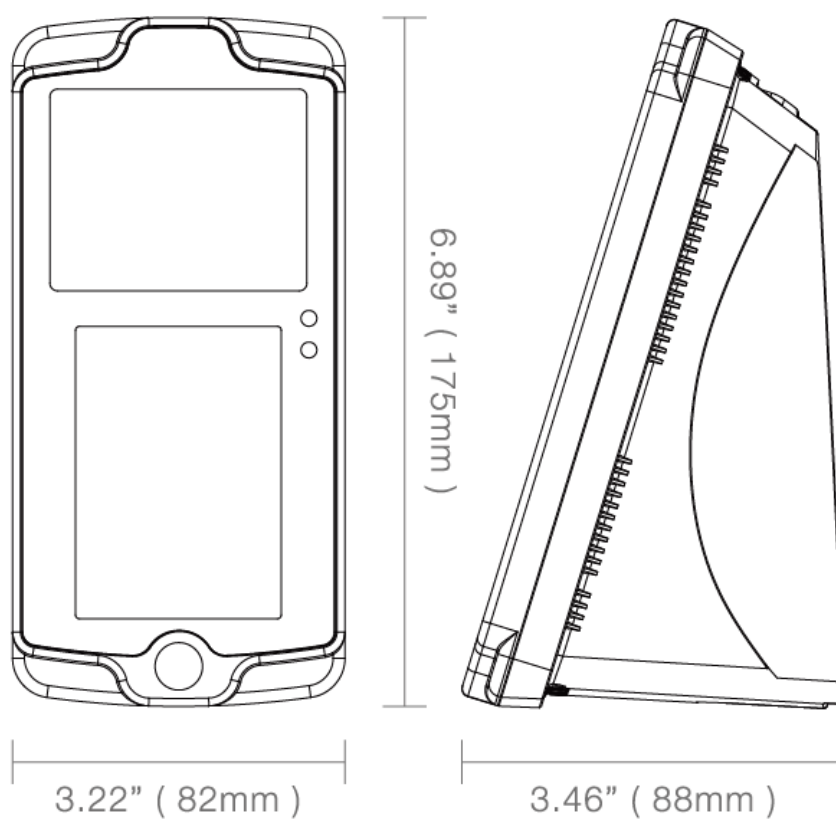


Figure 2-1: GHTER-XX Terminal

2.4 Maatvoering montageplaat

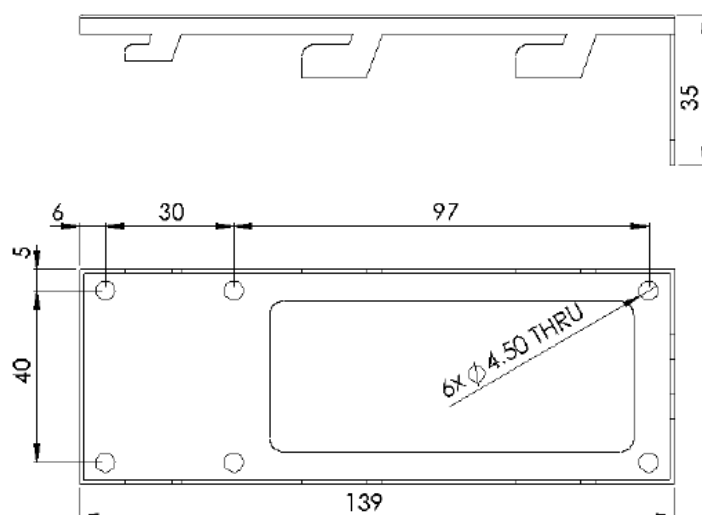


Fig. 2-2: Mounting Bracket (in mm)

2.5 GHTER-XX Port Pins and Switches

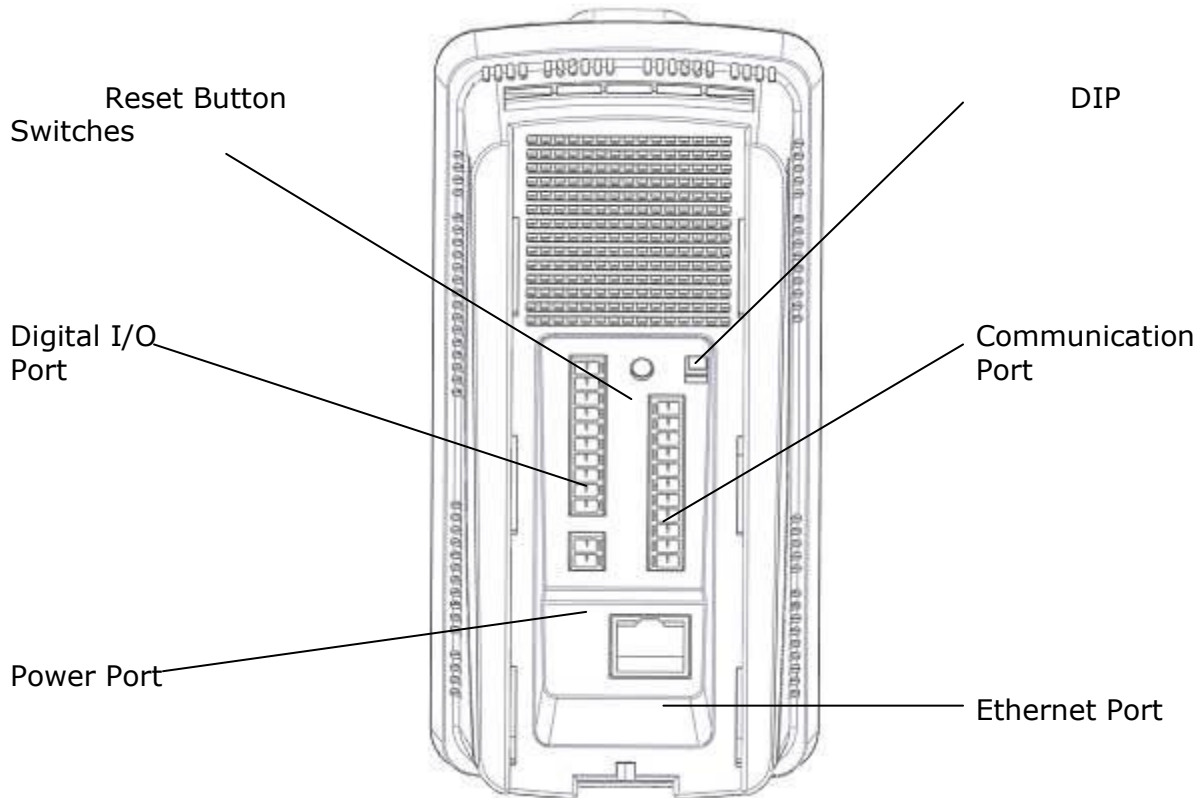


Fig. 2-3

Your GHTER-XX interface with other external hardware via a set of port pins. There is a set of buttons and switches to provide rudimentary user input functions. All pins and buttons are at the back of the GHTER-XX . See Fig. 2-3.

Each port pin and switch of your GHTER-XX Terminal is labeled according to Fig. 2-4.

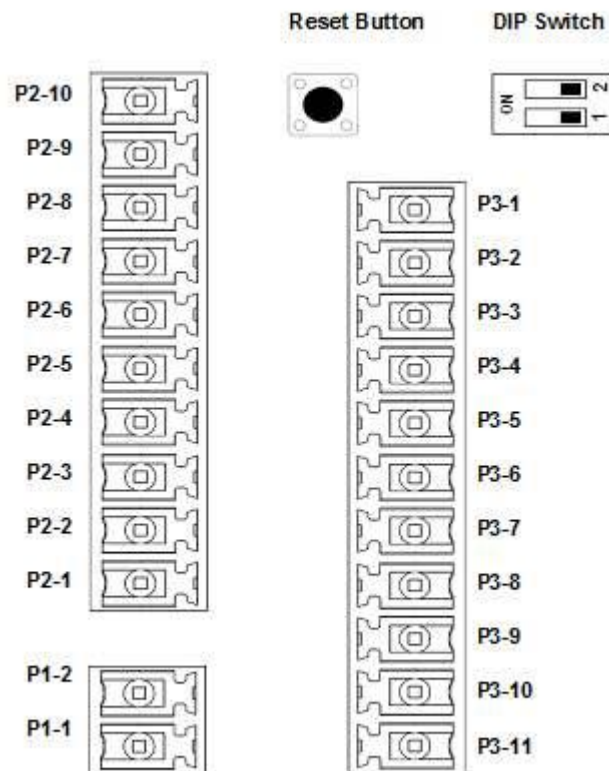


Fig. 2-4

2.6 DIP Switch

There is a two-position DIP switch used for system configuration. Position 1 is used to disable built-in access controller, as illustrated in Fig. 2-5. Position 2 is reserved for future use..



Built-in Controller Enabled



Built-in Controller Disabled

Fig. 2-5

When Position 1 is set ON, the built-in access controller interfaces, from P2-1 to P2-10, will be disabled.

2.7 Reset Button

Press the reset button of GHTER-XX Terminal three (3) times to set the system configuration to its factory default values. Once you press the button three times, the LCD will display a warning message informing the completion of reset. Then the system will reboot automatically and its IP Address is reinstated to the default value (192.168.1.100) after reboot. See Appendix for a summary of the factory default values.

2.8 Terminal Block Port Pins

The GHTER-XX terminal has three terminal block ports, located at the back of the unit, for power supply, digital I/O, and communication. Table 2-2 lists the definition for each port pin.

Table 2-2

| Product | AccuFACE® Terminal | |
|--------------------------|--------------------|-------------------|
| Port | Pin # | Definition |
| P1. POWER | 1 | 12V POWER SUPPLY |
| | 2 | 12V POWER GND |
| P2. DIGITAL I/O | 1 | DOOR SENSOR INPUT |
| | 2 | 12V DC OUT |
| | 3 | EXIT SWITCH INPUT |
| | 4 | 12V DC OUT |
| | 5 | RELAY 1 COM |
| | 6 | RELAY 1 N.C. |
| | 7 | RELAY 1 N.O. |
| | 8 | RELAY 2 COM |
| | 9 | RELAY 2 N.C. |
| | 10 | RELAY 2 N.O. |
| P3. COMMUNICATION | 1 | 12V POWER OUT |
| | 2 | 12V POWER OUT GND |
| | 3 | WIEGAND IN DATA0 |
| | 4 | WIEGAND IN DATA1 |
| | 5 | WIEGAND OUT DATA0 |
| | 6 | WIEGAND OUT DATA1 |
| | 7 | RS-232 TX |
| | 8 | RS-232 GND |
| | 9 | RS-232 RX |
| | 10 | RS-485 + |
| | 11 | RS-485 - |

2.8.1 • P1: Power Supply Port

This port is the 12VDC power supply port . The suggested rating is as follows:

- o 1000 mA for GHTER-XX if 12 VDC power output pins P3-1 and P3-2 are not used.
- o 2000 mA for GHTER-XX if 12 VDC power output pins P3-1 and P3-2 are used to power a device such as a card reader.

2.8.2 • P2: Digital I/O Port

- o P2-1 and P2-2 Door Sensor:

The door sensor is triggered when P2-1 detects a signal voltage of 5~24 VDC supplied by an external door sensor. You can use P2-2 (12 VDC out) to power the external sensor if necessary. The P2-1 is protected by a photo-coupler rated at 5 VDC/2.5 mA ~ 24 VDC/22 mA.

- o P2-3 and P2-4 Exit Switch:

The exit switch is triggered when P2-3 detects a signal voltage of 5~12 VDC supplied by an external exit switch. You can use P2-4 (12 VDC out) to power the external switch if necessary. The P2-3 is protected by a photo-coupler rated at 5 VDC/2.5 mA ~ 24 VDC/22 mA.

- o P2-5 to P2-7 Relay #1:

Relay #1 is a standard relay output interface with common (COM), normal close (N.C.), and normal open (N.O.) pins. The relay is rated at 2 A at 30 VDC and 1 A at 125 VAC.

- o P2-8 to P2-10 Relay #2:

Relay #2 is a standard relay output interface with common (COM), normal close (N.C.), and normal open (N.O.) pins. The relay is rated at 2 A at 30 VDC and 1 A at 125 VAC.

2.8.3 • P3: Communication Port

- o P3-1 and P3-2 12 VDC Power Output:

GHTER-XX Terminal can supply power to low-power peripherals such as card reader and keypad via P3-1 (12 VDC) and P3-2 (GND). If power supply on P1 is 2000 mA, the maximum output current is 1000 mA. Do not use these pins if your power supply on Port 1 is less than 2000 mA.

- o P3-3 to P3-6 Wiegand I/O:

Wiegand I/O pins are used to interface with an external device such as a card reader or keypad that can pass the user ID for facial authentication. P3-3 and P3-4 are the input pins, and P3-5 and P3-6 are the output pins.

- o P3-7 to P3-9 RS-232:

RS-232 is an expandable interface to communicate with a 3rd party device.

- o P3-10 and P3-11 RS-485:

RS-485 is an expandable interface to communicate with a 3rd party device.

2.9 Wiring Schematic

Your GHTER-XX has a built-in access controller. In default Internal Control Mode, electronic door lock and other peripheral devices such as card reader can be connected directly to GHTER-XX .

Alternatively a 3rd party access controller can be used in conjunction with your GHTER-XX. To enhance the physical security.

This section details the wiring schematic for Internal Control Mode in typical door lock control applications. Additional sections detail the status light and networking with your computer.

2.10 Typical Wiring Schematics

Fig. 2-6 shows the wiring schematic for the default mode in a typical door lock control application. Notice that some of the connection is optional.

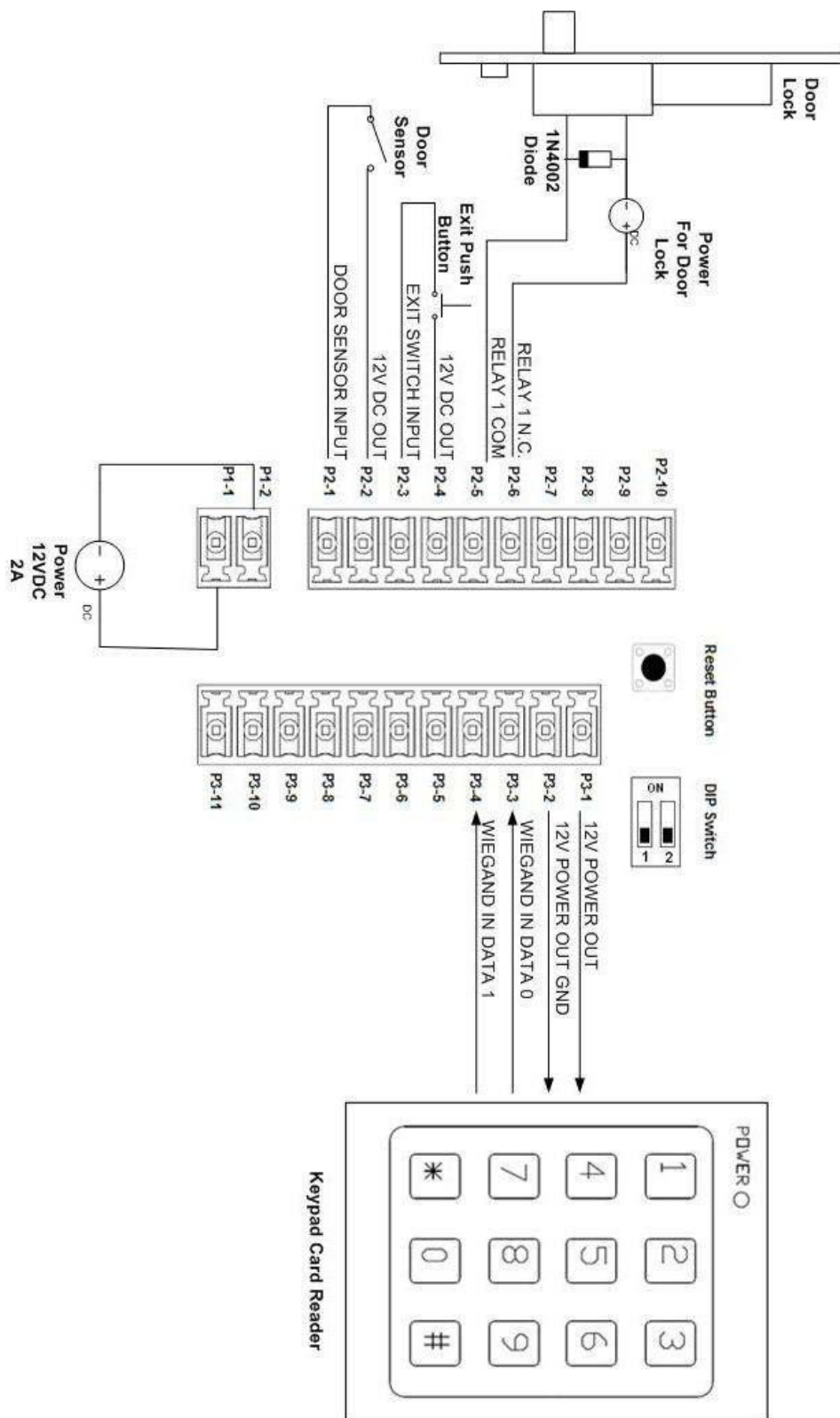


Fig. 2-6

- 12VDC power supply to P1-1 and P1-2.
- Door sensor to P2-1 and P2-2.
- Door exit switch to P2-3 and P2-4.
- Optional Wiegand output from Keypad Card Reader to P3-3 to P3-4.
- Optional power supply by GHTER-XX to Keypad Card Reader at P3-1 and P3-2.
- Optional RS-232 3rd party device to GHTER-XX P3-8 to P3-9.
- Ethernet cable to GHTER-XX LAN port. This is necessary only when doing user enrollment and system configuration from a PC.

Important Notes

It is a common practice to use different power supplies for the door lock and security controller. A sufficiently powerful door lock may draw enough current to adversely affect the power stability of the controller if both units share the same power source.

2.11 Turning On and Status Lights

Once you finished connecting GHTER-XX with external devices and communication cables, you can connect power supply to GHTER-XX . Since there is no ON/OFF switch , GHTER-XX powers up immediately with the connection of the power supply.

There are two status LEDs indicating the following status.

- Upper LED
 - o Flashing Green: GHTER-XX Terminal is booting up.
Normally it takes about 30~40 seconds to complete.
 - o Solid Red: Completion of boot up process. System is in operation.
- Lower LED
 - o Solid Red: Both relays (Relay #1 and Relay #2) are closed.
 - o Solid Green: Either Relay #1 or Relay #2 is open.

2.12 Networking with Computer

To access the network interface of GHTER-XX , you can connect GHTER-XX directly to your computer via an Ethernet crossover cable. Alternatively, you can connect GHTER-XX indirectly to your computer via a shared LAN network, wired or wirelessly. For wireless access, you need to connect your GHTER-XX to a wireless router as it does not equip with Wi-Fi interface. Access to your GHTER-XX from your computer is based on the device's assigned IP address. User may change the IP address if needed (see Chapter 3 for detailed instructions). A single computer can access multiple GHTER-XX as long as they are assigned to different IP addresses and share the same LAN network environment as the computer.

Important Notes

- 1) Default IP address is 192.168.1.100
- 2) Some computers' network ports do not support the feature of automatic crossover. Thus, a crossover CAT 5 Ethernet cable is highly recommended for peer-to-peer direct connection between GHTER-XX Terminal and computer.

3 Software Setup

Your GHTER-XX system is streamlined for easy operation and a complete network experience. Its built-in Web server allows you to access a Web-based administration interface from your computer via a standard Web browser (e.g. Internet Explorer, Firefox, Safari). The administration interface includes basic features for general system operations and advanced features to setup and customize your GHTER-XX for user-defined applications. This chapter discusses the following topics:

- Accessing GHTER-XX through web interface
- Basic features
- Advanced features
- Support

Before we start the discussion of the Web-based administration interface, please ensure your GHTER-XX and other hardware are properly setup. If not, please refer to Chapter 2.

3.1 Accessing GHTER-XX through Web Interface

You can initiate a communication link between your computer and your GHTER-XX by:

1. Power up your GHTER-XX according to the instructions provided in Chapter 2.
2. Using any PC in the same LAN environment, open a web browser and point it to <http://192.168.1.100>. This is the default IP address of your GHTER-XX which can be changed after the first log-in.

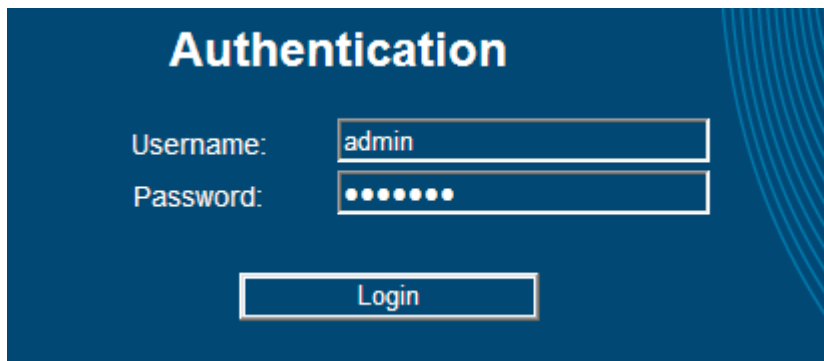


Fig. 3-1

3. Once connection is established, the browser should prompt you to enter your username and password. The default username is admin, and the default password is abcd1234. See Fig. 3-1 for a log-in screenshot. Please refer to Section 3.15 for details on changing username and password.

3.2 Basic Features

This section describes the basic configuration menus of your GHTER-XX device. The basic features are categorized into the following four groups.

- Status
- Log
- User management
- Schedule

3.3 Status

To view the status data, choose Basic -> Status on your web interface. A screenshot of the Status menu is shown in Fig. 3-2. The System Status page gives you the following system information:

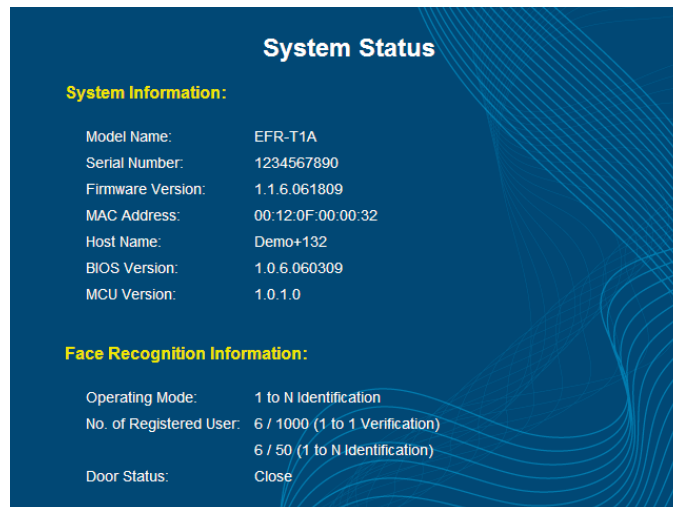


Fig. 3-2

- Model Name

This displays the model name of your GHTER-XX Terminal.

- Serial Number

This shows the serial number of your GHTER-XX Terminal. This number is unique on each device.

- Firmware Version

This shows the firmware version information.

- MAC Address

This displays the Media Access Control (MAC) address of the network interface.

- Host Name

This displays the host name of your GHTER-XX Terminal. The host name is a user defined alias name.

- BIOS Version

This displays the BIOS version of your GHTER-XX Terminal.

- MCU Version

This displays the MCU version of your GHTER-XX Terminal.

You can also find the following status information under facial recognition information.

- Operating Mode

This displays the current operating mode. This can be either 1: N identification or 1:1 verification.

- Number of Registered User

This displays the total numbers of registered users and maximum supported number of users for both 1: N identification mode and 1:1 verification mode.

- Door Status

This displays the current status of the door controlled by your GHTER-XX Terminal. Note that this status display is effective only when if the door sensor is enabled.

3.4 Log

To view or retrieve event log data, choose Basic -> Log. A screenshot of the Log menu is shown in

Fig. 3-3. The Log page allows you to configure the following options:

Fig. 3-3

- Log Display Method

To select the number of events displayed per page.

- Log Display Filter

To filter the displayed log events by date, user ID, image, or type.

o By Date: You can select the start and finish date to display all log events within the time period.

o By ID: You can view the log events associated with a selected user. You can either use the drop-down menu to select a user from the list, or directly enter the user ID.

o By Image: GHTER-XX can be programmed to take images for certain log events. You can select to view only log events that have images associated with them.

o By Type: You can select to view the log events based on Table 3-1 by checking on the associated boxes.

| | |
|-----------------------|-----------------------|
| User Enrolled | Authentication Passed |
| Authentication Denied | User Registered |
| User Removed | Unknown |
| Door Sensor Triggered | Card/User ID |
| Tamper Alarm | Exit Switch Triggered |
| Log-In Denied | Log-In Passed |
| Firmware Updated | Configuration Changed |
| System Boot-Up | EFR-API Connected |
| | Exiting Sleep Mode |

Table 3-1

Log messages:




| | Log Time | Description | Image |
|---|---------------------|---------------------------------|---|
| | 2009/12/16 10:29:09 | Configuration Changed | |
| | 2009/12/16 10:28:02 | Configuration Changed | |
| ✓ | 2009/12/15 14:32:47 | User 2987283058(Cary) is Passed |  |
| ✓ | 2009/12/15 14:31:49 | User 2987283058(Cary) is Passed |  |
| ✓ | 2009/12/15 14:31:26 | User 2987283058(Cary) is Passed |  |

Fig. 3-4

- **Clear Log button**

Click this button to permanently remove all log events. Notice that the maximum number of log events is specified in the latest product specification without prior notification.

- **Show Log button**

Once you have selected your preferences, click on the "Show Log" button to display the log events in a table format. See Fig. 3-4.

3.5 User Management

This menu allows you to enroll, upload, download, and remove users from GHTER-XX user database. Choose Basic -> User Management to access to this menu. A screenshot of this menu is shown in Fig. 3-5.

Fig. 3-5

The User Management page has these options:

- **Current Status**

To display the total numbers of registered users and maximum supported users for both 1: N identification mode and 1:1 verification mode.

- **Add User**

To add user to the user database, you can either enroll a new user, or upload an existing user.

Click on "Enroll," and you will see the facial enrollment page (see screenshot in Fig. 3-6). You will be prompted to enter the following data:

Facial Enrollment

Enrollment Information:

User ID: 1260988261 From Wiegand

User Name:

Number of Faces to Enroll:

Wear Glasses: No

User Type: Normal User

Quality Check Level: 5 (Mid)

Fig. 3-6

o User ID:

Each user must have a unique identification number. For 1:1 verification mode, the user ID is used to specify user identity before doing facial verification. The range of user ID is from 1 to 4294967295. You can also read ID number from a card via Wiegand Input interface by clicking on "From Wiegand" button.

o User Name:

The maximum number of characters is limited to 10. Only alphanumerical characters are supported.

o Number of Faces to Enroll:

To define the number of facial captures for this enrollment. Although the minimum number of facial captures is 10, we recommend you to use 12 facial captures so that you can delete 2 unwanted facial captures.

o Wear Glasses:

If the user wears glasses, select "Yes." Half way through the facial capture, GHTER-XX LCD on-screen display would remind user to remove the glasses to complete the facial capture.

o User Type:

Please refer to Table 3-2 regarding the supported user types and their authentication methods.

| User Type | Authentication Method |
|-------------|---|
| Normal User | Default user type; user needs to pass facial recognition to grant a pass result. |
| Root User | User with special privilege to enter the Standalone Mode (refer to Chapter 4 for more details). A system can have up to 3 root users. |
| Card Only | A special user type which |

| | |
|------------|--|
| | needs only card scan (or entering PIN) to grant a pass result. A Card Only user does not need to enroll facial templates in the system. |
| Card+Photo | A special user type similar with Card Only, but the user needs not only the card scan (or entering PIN), but also a photo snapshot to grant a pass result. A Card+Photo user does not need to enroll facial templates in the system. |

Table 3-2

o Quality Check Level:

Here, you select the quality level required for accepting a face capture during enrollment via a drop-down bar. The higher the level, the more accurate the face-print at the cost of a longer enrollment process. 5 (Mid) is the default and recommended setting.

o Start Enrollment:

Once the button is clicked, the enrollment process will begin. User positions the face in front of GHTER-XX to complete the facial capture. See Chapter 5 for a detailed description and suggestions of the enrollment process. The images captured during the enrollment process will be displayed, as shown in Fig. 3-7. Uncheck those unwanted images (e.g. poor image quality, serious reflection on glasses) to leave exactly 10 images, then click "Complete" button to finish the enrollment process.

o Cancel Enrollment:

Click this button to exit the enrollment. You may choose to exit anytime during the enrollment process.

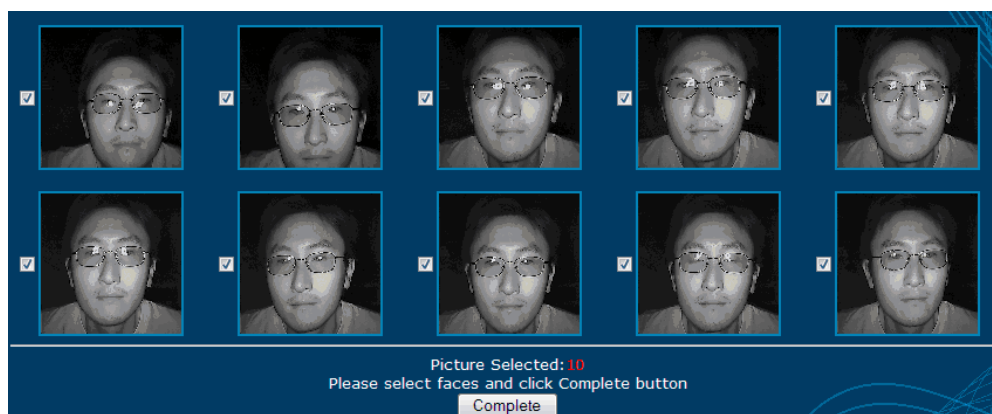


Fig. 3-7

● Upload User and Download User

A user's faceprint can be uploaded (from PC to GHTER-XX Terminal) and downloaded (from GHTER-XX Terminal to PC). These two features are useful when you need to backup the enrolled users, and when you need to duplicate the users on other GHTER-XX Terminals. The faceprint file name is the User ID, and the file extension is *.face. Note that a user's schedule information is also stored in the faceprint file.

● Remove User

To remove a specific user or all users from the user database.

- o **Remove Single User:** Select the user to be removed. Then click the "Remove" button to

- permanently remove that user from the user database.

- o **Remove All Users:** Click on the "Remove All" button to completely and permanently clear all users from the user database.

● User Database

You can manage and assign up to 50 users to 1:N group by clicking 'Edit' button of 'Users in 1 to N Identification:'. Similarly, you can assign up to 3 root users by clicking 'Edit' button of 'Root Users:'. In the User Database edit menu, you can click to select a user, then hit '<' or '>' buttons to move a user between groups.

3.6 Schedule

This menu allows you to edit the schedule for each user in the user database. Choose Basic -> Schedule to access to this menu. A screenshot of the Schedule page is shown in Fig. 3-8.

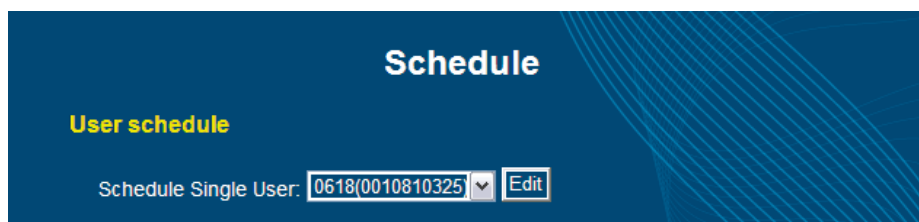


Fig. 3-8

Once the user is selected, you can edit the weekly schedule of the user. Each user can have up to 64 time slots (including a default policy), each with one of the following policies:

- Authentication: User needs to pass the facial recognition authentication to be able to pass during this time slot.
- Card Bypass (Card Only): Facial recognition is not required. User can pass the authentication with his/her card during this time slot.
- Always Deny: User is always denied during this time slot.
- Card + Photo: User can pass the authentication with a card scan along with a photo snapshot during this time slot.

Upon a user is enrolled, a default policy Authentication is applied during the whole week. You can generate more time slots with different policies according to the application needs.

3.7 Advanced Features

This section describes the advanced configuration menus of your GHTER-XX Terminal. The advanced features are categorized into 9 groups:

- Facial Recognition
- Network
- I/O Control
- Wiegand
- Display
- Log Configuration
- Time
- Password
- System
- Firmware

These parameters should be subject to minimal modification. Consult your installer if you are not certain about the setting of these parameters.

3.8 Facial Recognition

This menu allows you to set the facial recognition operating mode and recognition threshold.

Choose Advanced -> Facial Recognition to access to this menu. A screenshot of the facial recognition page is shown in Fig. 3-9.

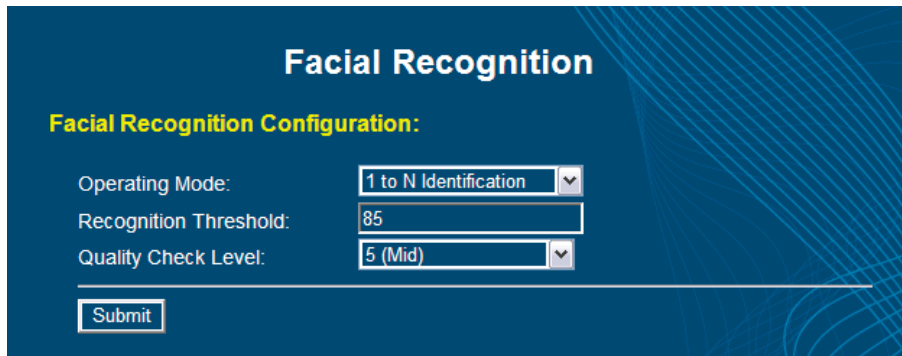


Fig. 3-9

• Operating Mode

User can select between 1:N identification and 1:1 verification modes via a drop-down bar. In 1:N identification mode, GHTER-XX identifies a face from all registered faces in the user database. In 1:1 verification mode, GHTER-XX receives a user ID from an external device (card reader, keypad) and verifies user face by comparing it with a registered facial record associated with the user ID.

• Recognition Threshold

The GHTER-XX facial recognition algorithm compares user face with enrolled facial template(s) and outputs a score. A higher score means a better match. The

recognition threshold option allows user to set a minimum score required to grant a face match a passing status. A low threshold increases recognition speed but also increases False Acceptance Rate (FAR) – the likelihood of mistakenly granting a passing status to an unregistered user. A high threshold, in contrast, reduces FAR but increases False Rejection Rate (FRR) – the likelihood of denying a registered user. The default recognition threshold of 85 is recommended for optimal FAR and FRR. The maximum threshold should not exceed 90 to avoid high FRR.

• Quality Check Level

Here you select the quality level required for accepting a face capture during the authentication. The higher the level, the more accurate the face-print at the cost of a longer authentication process. 5 (Mid) is the default and recommended setting. If a faster and smoother authentication process is required, please assign it to 4 or smaller number.

3.9 Network

Here, you can customize the networking configuration by choosing Advanced -> Network to access to this menu. A screenshot of Network page is shown in Fig. 3-10. In the Network page, the IP address of GHTER-XX is displayed. Other network configuration options are discussed below:

Fig. 3-10

• DHCP Function

You can enable or disable the DHCP function. When the DHCP is enabled, the system will ignore the static IP address and fetch a dynamic IP Address from the DHCP server. Note that this feature is disabled in current firmware.

• Static IP Address

You can configure a static IP address for your GHTER-XX . It is your responsibility to avoid IP address conflict with other network devices in a shared network environment.

- **Static IP Netmask**

You can configure the static IP netmask here.

- **Static IP Gateway**

You can configure the static IP gateway here.

- **DNS Address**

You can configure the DNS (Domain Name Server) address here.

The following options are listed under the Internet Configuration.

- **Web Port**

You can configure the web port of your computer used to interface with the web-based administration interface here. Note that this feature is disabled in current firmware.

- **Firewall Level**

You can configure the firewall level to low, mid, or high level using the drop-down bar.

Note that this feature is disabled in current firmware.

- **Host Name**

You can change the host name, which is an alias name, of your GHTER-XX Terminal here.

3.10 I/O Control

Here, you can control the I/O (input and output) settings. Choose Advanced -> I/O Control to access this menu. A screenshot of the I/O page is shown in Fig. 3-11.



| I/O Control | |
|---------------------------------------|----------|
| Door Sensor Alarm: | Disabled |
| Door Sensor Polarity: | Normal |
| Door Sensor Alarm Time: | 30 |
| Exit Switch: | Enabled |
| Relay #1: | Enabled |
| Relay #1 Delay Time: | 0 |
| Relay #1 Open Time: | 5 |
| Relay #2: | Enabled |
| Relay #2 Delay Time: | 0 |
| Relay #2 Open Time: | 5 |
| <input type="button" value="Submit"/> | |

Fig. 3-11

You have control over the following I/O options:

- **Door Sensor Alarm**

This option should be enabled only if you have an electronic door lock with a door sensor output connected to the sensor pin P2-1 of your GHTER-XX Terminal. You can enable or disable the door sensor function via the drop-down bar.

- **Door Sensor Polarity**

Your external door sensor may generate a high or low signal upon activation. You should adjust this field to match the signal output of your door sensor. Use the drop-down bar to select between normal and inverse signal transition types. In normal signal transition, a P2-1 voltage above 3 V and 0 V are read as Door Closed and Door Open, respectively. In inverse signal transition, the interpretation is reversed.

- **Door Sensor Alarm Time**

GHTER-XX can be programmed to trigger an alarm and log an event if the door is open for over a pre-defined time limit. Type the alarm time limit in seconds. Note the default time is 30 seconds.

- **Exit Switch**

Enable this option if you have an exit switch connected to your GHTER-XX Terminal that allows you to open an electronic door lock when the switch is activated.

- **Relay #1**

You can enable or disable Relay #1 control signals (N.C and N.O.) here. When enabled, Relay #1 will engage when a user is granted a "Passed" status.

- **Relay #1 Delay Time**

You can set the time delay (in second) between the moment a user is granted a "Passed" status and the moment of engagement of Relay #1. The default value is zero second for no delay.

- **Relay #1 Open Time**

You can set the duration of the engagement of Relay #1 after the user is granted a "Passed" status. You can type the open time in seconds. The default value is 5 seconds.

You can configure Relay #2 in the same manner as Relay #1. Once you are ready, click on the "Submit" button, and the changes take effect immediately.

3.11 Wiegand

Here, you can control the Wiegand settings by choosing Advanced -> Wiegand menu. A screenshot of Wiegand page is shown in Fig. 3-12. GHTER-XX can interface with other peripherals using standard Wiegand protocols to perform multi-factor authentication. Furthermore, GHTER-XX can also act as a standard Wiegand Output device to interface with other controllers. You can adjust various Wiegand protocol parameters in the Wiegand page.

Fig. 3-12

● Wiegand Input

To enable or disable the Wiegand input function.

● Wiegand Input Format

You can use the drop-down menu to choose Standard 26-bit, or Standard 34-bit for the Wiegand input protocol format.

● Wiegand Output

To enable or disable the Wiegand output function.

● Wiegand Output Format

You can use the drop-down menu to choose Standard 26-bit, or Standard 34-bit format for the Wiegand output protocol format.

Once you complete the configurations, click the "Submit" button, and the changes take effect immediately.

3.11.1 Defining Custom Format for Wiegand Input Interface

Objective

GHTER-XX has two built-in Wiegand input formats -- Standard 26-bit and Standard 34-bit that are commonly supported by regular card reader devices. However, for security or other management concern, there're still many special Wiegand formats with different lengths and bit arrangement applied in real-world integrations.

In order to support those special formats, GHTER-XX supports an interface where you can easily define your proprietary Wiegand input format, of up to 64 bits.

Instructions

On the Web administration interface, goes to **Advanced>Wiegand** page. In the Wiegand Input Format section, select "Custom Format" then a edit box below it will become active. By default, the edit box is empty; you can edit your own string of custom format based on below rules. Once completed, click Submit button and it will take effect instantly.

| Letter | Definition | Remark |
|--------|---------------------------------------|-----------------------------|
| U | MSB (Most Significant Bit) of User ID | A upper-case U |
| u | A bit of User ID | A lower-case u |
| 0 | A bit must be 0 | |
| 1 | A bit must be 1 | |
| X | A don't care bit | Lower-case x works the same |

Rules and Limitations:

Max length of Wiegand bits: 64 bits

Min length of Wiegand bits: 4 bits

Max length of User ID: 32 bits (Including A "U" and a number of "u")

No undefined letter should be included in the string

A User ID string should either start with a "U" or end with a "U". A User ID string without "U" is not able to work Parity bits are not checked in current design of custom format string. User should always mark them as "X" (don't care) bits.

Example 1:

For scanning cards with 26-bit Wiegand code with a fixed Facility ID of 74 (01001010b), the Wiegand format is

P-FFFF-FFFF-Uuuu-uuuu-uuuu-uuuu-P

Where P are the Parity bits

F are the 8-bit Facility ID bits

U is the MSB of 16-bit User ID

u are the later 15 bits of 16-bit User ID,

So the string of custom format should be set as:

X01001010UuuuuuuuuuuuuuuuuX

Example 2:

For scanning cards with 34-bit Wiegand code with User ID from bit 2 to bit 17 in reversed bit order, the Wiegand format is

1-uuuu-uuuu-uuuu-uuuU-FFFF-FFFF-FFFF-FFFF-0

Where 1 is the leading bit, always 1

U is the MSB of 16-bit User ID

u are the later 15 bits of 16-bit User ID

F are the 16-bit Facility ID, which are don't care in this application

0 is the ending bit, always 0

So the string of custom format should be set as:

1uuuuuuuuuuuuuuuuUXXXXXXXXXXXXXXXXXX0

Example 3:

For scanning cards with 36-bit Wiegand code with a fixed Facility ID of 255 (FF hex)

PFFFFFFFFFFFFFFFFUuuuuuuuuuuuuuuuuXXP

X000000001111111UuuuuuuuuuuuuuuuuXXX

Example 4:

For scanning cards with 54-bit Wiegand code with a fixed Facility ID of 255 (FF hex)

PXXXXFFFFFFFFFFFFFFFFUuuX

XXXXX000000001111111UuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuuX

Error Formats

If the string of custom format is not well defined according the rule mentioned above, the Wiegand input will be ignored by GHTER-XX without notice. Below are a few typical examples of wrong format.

| String of Custom Format | Reason of Error |
|----------------------------|-------------------------------------|
| X01001010uuuuuuuuuuuuuuuuX | No MSB "U" is assigned |
| X01001010uuuuuuuuuuuuuuuuX | More than 1 "U" is assigned |
| XpXXXXXXXXUuuuuuuuuuuuuuuX | An undefined letter "p" is included |
| X01001010 UuuuuuuuuuuuuuuX | A space is in between |

3.12 Display

Here, you can control the display settings of your GHTER-XX . Choose Advanced -> Display to access to this menu. A screenshot of the Display page is shown in Fig. 3-13.

This menu allows you to enable or disable the face marker. The face marker is a rectangular frame that tracks your facial movement. Simply select enable or disable in the drop-down menu of the Draw Face Marker option. Once you are ready, click the "Submit" button, and the changes take effect immediately.

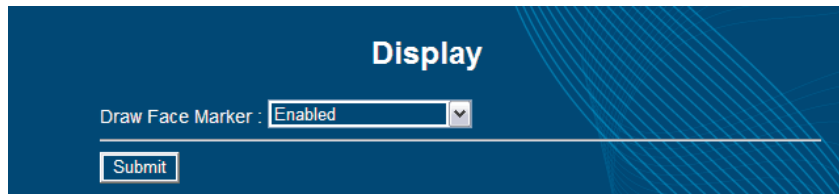


Fig. 3-13

3.13 Log Configuration

Here, you can control the log configuration settings of your GHTER-XX . Choose Advanced -> Log Configuration to access to this menu. A screenshot of Log Configuration is shown in Fig. 3-14.

You can choose which events to log. The log events can be categorized as follows. The facial recognition log events are as follows.

- User enrolled
- Authentication passed
- Authentication denied
- User registered
- User removed
- Unknown card maker
- Unknown card/user ID

The input/output log events are as follows.

- Door sensor triggered
- Exit switch triggered
- Tamper alarm

Network log events are as follows.

- Log-in passed
- Log-in denied
- Configuration changed
- Firmware updated
- EFR-API connected

System log events are as follows.

- System boot-up
- Exit sleep mode

Log Configuration

Facial Recognition:

| | |
|------------------------|--|
| User Enrolled: | <input type="text" value="Log Message and Image"/> |
| Authentication Passed: | <input type="text" value="Log Message and Image"/> |
| Authentication Denied: | <input type="text" value="Log Message and Image"/> |
| User Uploaded: | <input type="text" value="Log Disabled"/> |
| User Removed: | <input type="text" value="Log Disabled"/> |
| Unknown Card/User ID: | <input type="text" value="Log Message"/> |

I/O Control:

| | |
|------------------------|--|
| Door Sensor Triggered: | <input type="text" value="Log Message"/> |
| Exit Switch Triggered: | <input type="text" value="Log Message"/> |
| Tamper Alarm: | <input type="text" value="Log Message"/> |

Network:

| | |
|------------------------|---|
| Login Passed: | <input type="text" value="Log Disabled"/> |
| Login Denied: | <input type="text" value="Log Message"/> |
| Configuration Changed: | <input type="text" value="Log Message"/> |
| Firmware Updated: | <input type="text" value="Log Message"/> |
| EFR-API Connected: | <input type="text" value="Log Disabled"/> |

System:

| | |
|---------------------|---|
| System Bootup: | <input type="text" value="Log Message"/> |
| Exiting Sleep Mode: | <input type="text" value="Log Disabled"/> |

Fig. 3-14

All log events allow you to select to log message or disable completely via a drop-down menu. Some log events also allow you to log the image where the captured image associated with the event is logged. Once you are ready, click the "Submit" button, and the changes take effect immediately.

Time

Synchronize System Time

☒ with PC ☐ with Manual Input Time

| | | | | | |
|-------|-----------------------------------|---------|---------------------------------|---------|---------------------------------|
| Year: | <input type="text" value="2009"/> | Month: | <input type="text" value="6"/> | Day: | <input type="text" value="23"/> |
| Hour: | <input type="text" value="01"/> | Minute: | <input type="text" value="46"/> | Second: | <input type="text" value="27"/> |

Fig. 3-15

3.14 Time

Here, you can control the time settings of your GHTER-XX . Choose Advanced -> Time to access this menu. A screenshot of Time page is shown in Fig. 3-15. You have the option to synchronize the system date/time with your PC or inputting the date/time manually. Once you are ready, click the "Submit" button, and the changes take effect immediately.

Important Notes

Once GHTER-XX terminal is removed from the mounting bracket and rebooted, the memory of its internal clock will be lost. The system clock will be reset to its factory default time and date. The mounting bracket works as an activator of real-time clock (RTC) battery. Once you mount the GHTER-XX securely to the mounting bracket, be sure to boot it up and configure the time.

3.15 Password

Here, you can control the password settings of your GHTER-XX . Choose Advanced -> Password to access this menu. A screenshot of Password page is shown in Fig. 3-16. Fig. 3-16

You can modify the following password settings:

Password

Administrator Username:

Administrator Password:

User 1 Username:

User 1 Password:

User 2 Username:

User 2 Password:

User 3 Username:

User 3 Password:

Passcode:

3.15.1 Admin Username and Password

To enter the administrator username and password. The administrator can access the Webbased administration interface. The default user name is "admin" and the default password is "abcd1234".

3.15.2 User Username and Password

You can enter the username and password for up to 3 users. The default names are "user1", "user2", and "user3" and their passwords are all empty. These 3 users will not be active unless appropriate passwords are assigned here.

3.15.3 Passcode

Passcode is a 4-digit numeric code used for initiating Standalone Mode from Wiegand keypad. Default Passcode is '1234', and you can change the Passcode to further enhance the security. Please refer to Chapter 4 for more information regarding Standalone Mode.

3.15.4 System

Here, you can control system settings of your GHTER-XX . Choose Advanced -> System to access this menu. A screenshot of System page is shown in Fig. 3-17.

3.15.5 Power Saving Time

Use the drop-down menu to select a system idle time before switching to power-saving mode where most of the IR LED and the LCD panel are turned off. Your GHTER-XX will stay in power-saving mode until it detects motion (in 1:N identification mode) or a system event occurs (e.g. Wiegand input, exit switch, etc). Default idle time is 10 seconds.

3.15.6 Motion Detector Sensitivity

In power-saving mode, GHTER-XX can detect motion within a pre-defined range. You can adjust the motion detector range by adjusting the sensitivity from 1 to 9 (1 is the minimum and 9 is the maximum).

3.15.7 Display Language

You can use the drop-down bar to select your preferred language display. The language preference will apply to both On-Screen Display (OSD) interface on LCD panel and Webbased administration interface.

Once you are ready, click the "Submit" button, and the changes take effect immediately.

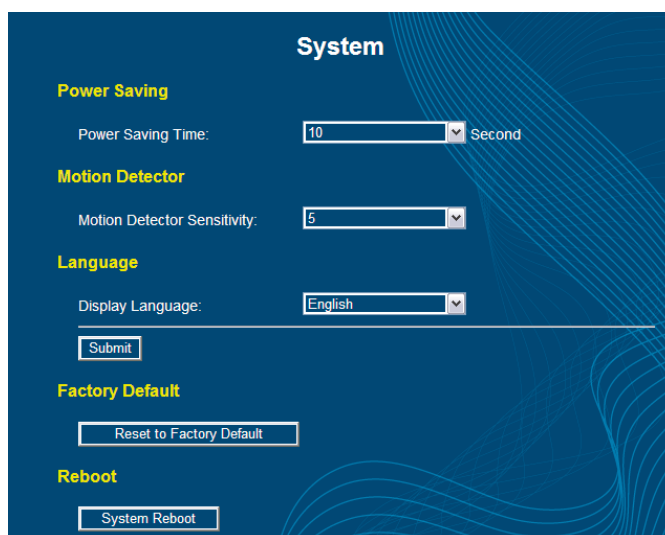
The image shows a web-based configuration interface for a system, titled "System". It features a dark blue background with a subtle pattern of white wavy lines. The interface is organized into sections: "Power Saving" with a "Power Saving Time" dropdown set to "10" and the unit "Second"; "Motion Detector" with a "Motion Detector Sensitivity" dropdown set to "5"; "Language" with a "Display Language" dropdown set to "English"; a "Submit" button; "Factory Default" with a "Reset to Factory Default" button; and "Reboot" with a "System Reboot" button. All buttons and dropdown menus are white with black text.

Fig. 3-17

In addition, you can choose to reset the system to factory default settings by clicking the "Reset to Factory Default" button. Note that this process is irreversible. You can also choose to reboot your GHTER-XX by clicking on the "System Reboot" button. The system will shut down and reboot.

3.16 Firmware

Here, you can check the current firmware version of your GHTER-XX and upload the latest firmware to your GHTER-XX . Choose Advanced -> Firmware to access this menu. A screenshot of Firmware page is shown in Fig. 3-18.



Fig. 3-18

To update a new firmware, first click the "Browse" button to select the path of the desired firmware file (*.bin or *.firmware file) to be uploaded. Then click the update button to initiate the firmware update procedure. You need to wait for a few minutes for the system to reboot to complete the firmware update process.

4 Standalone Mode

GHTER-XX is an embedded system that requires no external computer to operate. In this chapter, we are going to discuss the following topics:

- How to Use a Keypad in Standalone Mode
- Operations in Standalone Mode
- Menus of Standalone Mode

4.1 How to Use a Keypad in Standalone Mode

To operate GHTER-XX Terminal in the Standalone Mode, users have to understand the definition of each key on a keypad.

- o *** : Enter Key** – When a number (one or several digits) is input, you need to press * (Enter Key) to confirm the command.
- o **# : Clear Key** – When a wrong number is entered, you can press # (Clear Key) to clear all previous digits.
- o **0~9: Number Key** – The function of each number key is displayed in the menu on LCD screen.
 - In a menu which needs an input of single digit number, press single number key followed by Enter Key to proceed.
 - In most of the menus, you can press 0 followed by Enter Key to go back to the previous layer of menu.
 - In a menu which have multiple pages of information (e.g. Log Display), you can enter 9 followed by Enter Key to go to the next page, and enter 7 followed by Enter Key to go to the previous page.
 - In a menu which needs an input of multiple digit number (e.g. User ID), enter all digits and a Enter Key to confirm it.

4.2 Operations in Standalone Mode

In this section, we are going to know:

- Enter Standalone Mode for the very first time
- How to enroll
- Enter Standalone Mode after the first root user enrollment

4.3 Enter standalone mode for the very first time

To get into Standalone Mode for the very first time, or when no root user is present, enter the Passcode (default: 1234, followed by Enter Key), and you can enter Standalone Mode and a menu as shown in Fig. 4-1 will appear right away.

- (1) Status
- (2) Log
- (3) User
- (4) Setup
- (0) Back

Fig. 4-1

4.4 How to enroll

Once you enter Standalone Mode, enter "User" menu and choose "Enroll" to enroll a new user. You need to enter the new user's User ID, by entering it with the keypad, or by scanning the new user's proximity card. Then you need to choose one of the four user types: "Normal User," "Root User," "Card Only," or "Card + Photo". If no root user is enrolled, it is strongly recommended to enroll a root user to prevent unauthorized users to enter the Standalone Mode. On the "Wear Grass" page, the users who wear glasses select "Yes", whereas the users without glasses select "No." If a user selects "Yes," GHTER-XX LCD on-screen display will remind user to remove the glasses on half way through the facial enrollment.

On "Check Level" page, press the quality level (Rang 1 to 9) required for accepting a face capture during enrollment. The higher the level is, the more accurate the face-print at the cost of a longer enrollment process. On "Start Enroll" page, choose "Yes" to start enrollment. See Chapter 5 for a detailed description and suggestions of the enrollment process.

4.5 Enter Standalone Mode after the first root user enrollment

When more than one root user is enrolled, it needs root user's facial recognition to enter the Standalone Mode. To do so, please enter the Passcode (default: 1234, followed by Enter Key). After a red lock symbol appears on the upper right site of LCD display, the root user needs to complete the facial recognition.

In Fig. 4-2, it shows the screen of waiting a root user's facial recognition in 1:1 Mode. In Fig. 4-3, it shows the screen of waiting a root user's facial recognition in 1:N Mode.



Fig. 4-2

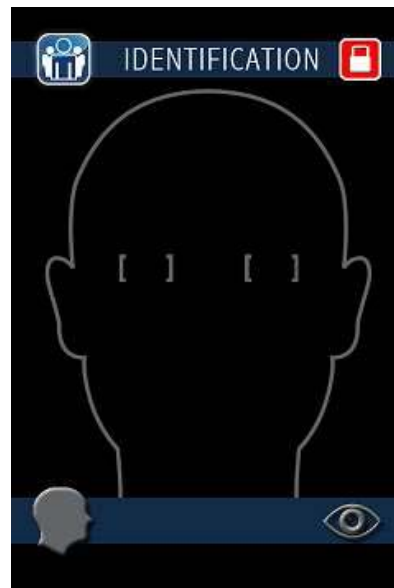


Fig. 4-3

Once a root user's facial recognition is passed, you will see the Standalone Mode menu as shown in Fig.4-1. For more description and suggestions for facial recognition process, please refer to Chapter 5.

4.6 Menus of Standalone Mode

This section describes the administration menus of the Standalone Mode. The administration menus are categorized into the following four groups:

- Status
- Log
- User
- Setup

4.7 Status

- **MODEL: Model Name**

This displays the model name of your GHTER-XX Terminal.

- **SN: Serial Number**

This shows the serial number of your GHTER-XX Terminal. This number is unique on each device.

- **FW VER: Firmware Version**

This shows the current firmware version information.

- **MAC: MAC Address**

This displays the Media Access Control (MAC) address of the network interface.

- **IP: This shows the current IP address.**

- **BIOS: BIOS version**

This displays the BIOS version information.

- **MCU: MCU version**

This displays the MCU version information.

- **USER: number of registered user**

This displays the total numbers of registered users and maximum supported number of users for both 1: N identification mode and 1:1 verification mode.

4.8 Log

- **Show All**

"Show all" is to list the entire log events.

- **Show Today**

Choose "Show Today" to list the log events only of today.

- **Show Critical**

"Show critical" list the critical log events, including "User Enrolled", "Authentication Denied" and "Tamper Alarm" events.

- **Clean All**

To permanently remove all log events.

4.9 User

- **List user**

To list all the users' ID here.

- **Enroll**

Please refer to Sec. 4.2.2 for the instructions.

- **Delete**

To remove a specific user from the user database. You need to manually input the User ID or scan the card of a specific user to remove it.

- **Delete all**

To delete all users from the user database. Note that this is an irreversible command. Please use it with care.

4.10 Setup

- **FR Mode**

Enter FR (Facial Recognition) menu to select between 1:N identification and 1:1 verification modes. In 1:N identification mode, GHTER-XX identifies a face from all registered faces in the user database. In 1:1 verification mode, GHTER-XX receives a user ID from an external device (card reader, keypad) and verifies user face by comparing it with a registered facial record associated with the user ID.

- **FR Threshold**

In FR Threshold menu, set a minimum score required to grant a face match a passing status.

The GHTER-XX facial recognition algorithm compares user face with enrolled facial template(s) and outputs a score. A higher score means a better match. A low threshold increases recognition speed but also increases False Acceptance Rate (FAR) – the likelihood of mistakenly granting a passing status to an unregistered user. A high threshold, in contrast, reduces FAR but increases False Rejection Rate (FRR) – the likelihood of denying a registered user. The default recognition threshold of 85 is recommended for optimal FAR and FRR. The maximum threshold should not exceed 90 to avoid high FRR.

- **Time**

Enter "Time" menu to input the date and the time manually.

- o Date Setting - Year: Range: 09 – 18: Year 2009 ~ 2018
- o Date Setting - Month: Range: 01- 12
- o Date Setting - Day: Range: 01- 31
- o Time Setting - Hour: Range: 00 – 23
- o Time Setting - Minute: Range: 00 – 59
- o Time Setting - Second: Range: 00 – 59

Once all date and time settings are entered, it will take 3~5 seconds to take effect.

- **I/O**

Access I/O (input and output) menu to configure the I/O settings.

- o Relay1/Relay2 Open Time

Set the duration of the engagement of Relay1 or Relay 2 after the user is granted a "Passed" status. You can type the open time in seconds.

The default value is 5 seconds. Acceptable range is 3~60 seconds.

- **Passcode**

Here, you can change the Pass code to enhance system security. The default

Passcode is 1234. To change the Passcode, you need to enter the old Passcode and then enter the new Passcode twice to confirm the change.

- **Reboot**

To reboot the GHTER-XX Terminal. Once selected, the system will beep 3 times and have the warm reboot.

5 Facial Enrollment and Recognition

Your GHTER-XX is equipped with Facial Positioning Guidance Interface (FPGI) which assists user to properly position his or her face for enrollment and recognition. This chapter explains the operations of FPGI interface, user enrollment and user recognition.

5.1 Enrollment

Chapter 3 describes how you can initiate the enrollment process from the Basic menu. This section will describe the actual enrollment process and how to use FPGI.

When the enrollment screen is displaying on your web browser, the LCD displays the screen shown in Fig. 5-1 to indicate it is in enrollment mode.



Fig. 5-1

Then the OSD will immediately switch to the screen shown in Fig. 5-2 showing a real-time camera display. At this point, you should position your face in front of the GHTER-XX Terminal.

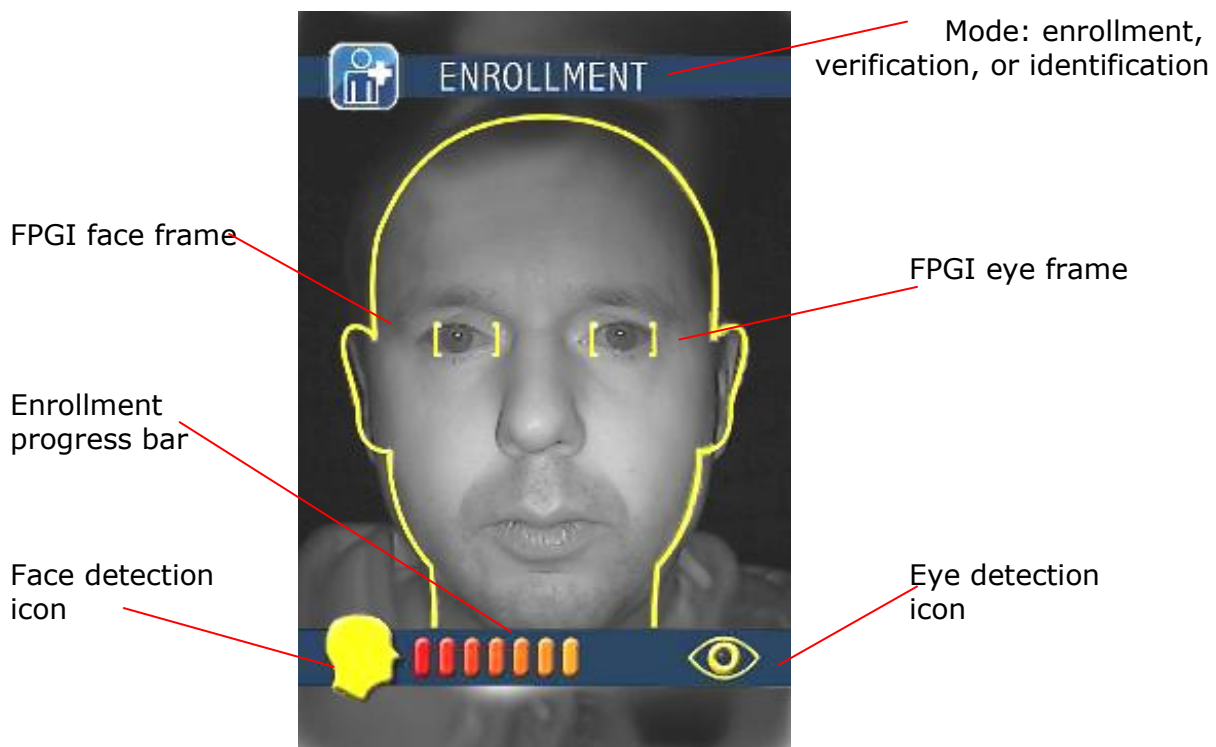


Fig. 5-2

The top of the OSD shows which operation mode GHTER-XX is in. Operation modes include Enrollment, Verification (1:1), and Identification (1:N). See Section 5.2 for details about 1:1 verification and 1:N identification. The enrollment progress bar, face detection icon, and eye detection icon are at the bottom of the OSD. The enrollment progress bar, at the bottom of the OSD, shows percentage of enrollment completion. The face and eye icons, as part of the FPGI, are explained below.

Facial Positioning Guidance Interface (FPGI) consists of a face frame and two eye frames and they are displayed in grey color on the OSD. Gently move your head so that your face and eyes are within the head and eye frames. Then the frames will turn into yellow color. GHTER-XX captures and enrolls user face only when the FPGI frames turn from grey to yellow. Upon a face image is successfully captured, you will hear a beep sound. User who wears glasses would be asked to remove the glasses in the middle of the enrollment process. Depending on your head placement, the OSD may also recommend you to move closer or further away from the GHTER-XX Terminal, as shown in Fig. 5-3. Please follow these guidelines to achieve the good enrollment:

- 1 Maintain your head within the FPGI frames (head and eye frames) during enrollment
- 2 Move your head closer and away from the GHTER-XX terminal and repeat this action 2-3 times.
- 3 Slightly nod your head up (no more than 15 degree) and move your head closer and away from the terminal and repeat this action 2 to 3 times.

- 4 Slightly nod your head down (no more than 15 degree) and move your head closer and away from the terminal and repeat this action 2 to 3 times.
- 5 If enrollment process is not complete, slightly turn your head left/right (no more than 15 degree) and move your head closer and away from the terminal and repeat this action 2 to 3 times.

If GHTER-XX is unable to capture all required face images within 60 seconds, a "Failed" message will be displayed on the OSD. Upon completion of the enrollment process, the OSD will show a "Done" message. See Fig. 5-4. Then the Web-based administration interface on your PC will display all the captured images. Check the ones that you wish to use for enrollment purposes and click "Complete" to complete the enrollment process.



Fig. 5-3

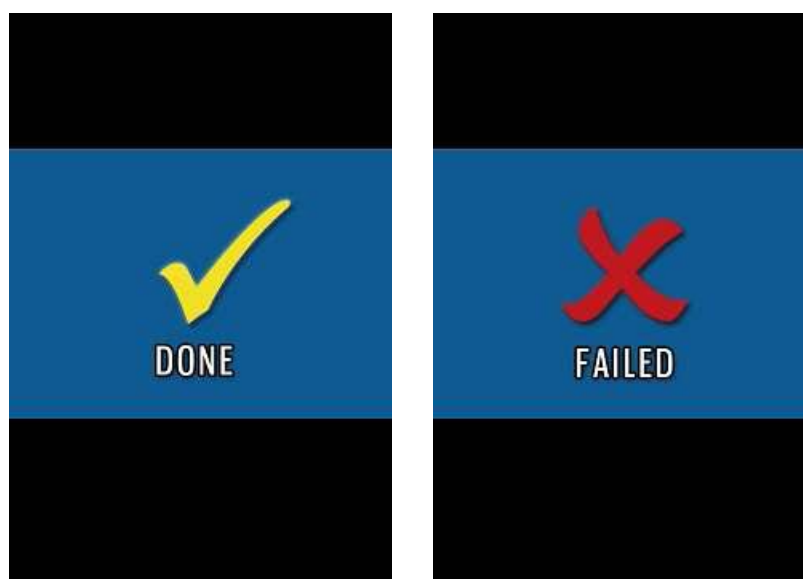


Fig. 5-4

5.2 Recognition

GHTER-XX facial authentication can operate under 1:N identification or 1:1 verification mode. See Chapter 3 for further details.

In 1:N identification mode, you simply stand in front of GHTER-XX (ensure you see your face within the FPGI frames) and allow your face to be scanned.

In 1:1 verification mode, GHTER-XX requests you to present your other identification (e.g. proximity card, pin code) first before allowing your face to be scanned (see Fig. 5-5). The user ID is received from a card reader or keypad through Wiegand interface, or from EFR-API commands.

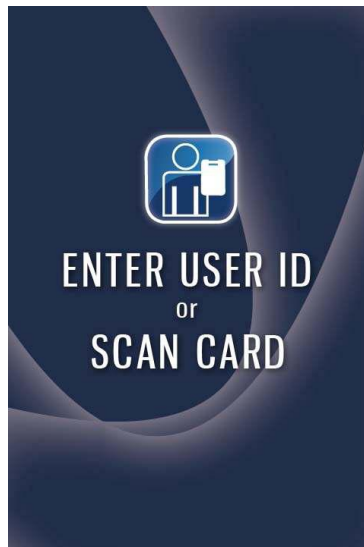


Fig. 5-5

GHTER-XX displays its operation mode (Identification or Verification) at the top of the OSD. See Fig. 5-6.

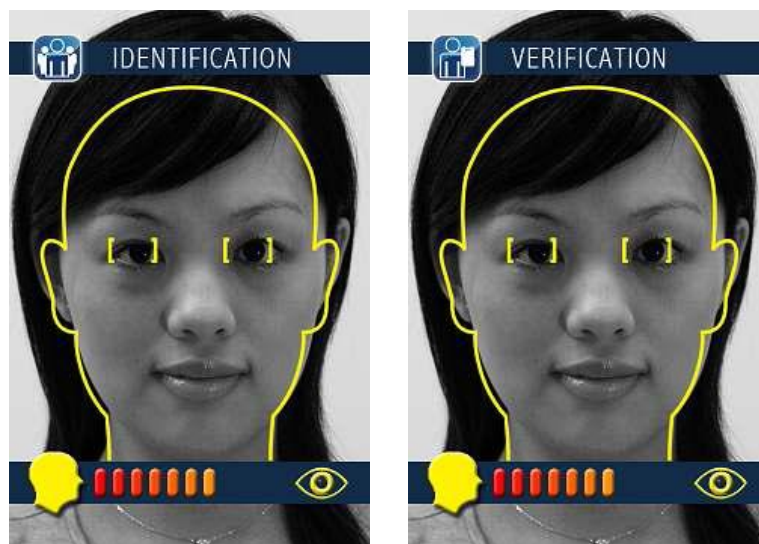


Fig. 5-6

The use of FPGI recognition is similar to that of FPGI enrollment. After face images were scanned and processed, GHTER-XX displays either a "Passed" or "Denied" message. See Fig. 5-6 and 5-7.



Fig. 5-7

There are some slight differences in the OSD message when compared with the enrollment case.

- The top of the OSD may display "Verification" or "Identification" (depends on your selection under Basic->Face Recognition->Operating Mode in the Web-based administration interface).
- During the facial authentication, the progress bar at the bottom of the OSD represents the real-time recognition score. For a registered user, if the face is well positioned, the progress bar will reach its maximum and the system will response with a "Pass".
- Upon successful recognition, OSD displays a score, user ID number, and user name under the "Pass" message.

6 Troubleshooting

If you encounter problem while using your GHTER-XX , this chapter may help! It discusses some frequently asked questions and our proposed solutions. A key to troubleshooting is to understand and remember the steps you went through prior to encountering the problem. Note the following when troubleshooting.

- Problems that occurs only with a specific application suggests that the application is not compatible with the installed version of GHTER-XX firmware.
- Some third-party external devices may not be compatible with your GHTER-XX .

If you are unable to solve your problems after reading and following the instructions in this chapter, Please contact your installer or alternatively the ARAS Security Technical Support Desk.

- My GHTER-XX does not turn on or start up.

Make sure the power adaptor is plugged into a functioning power outlet. Use a power adaptor that provides 12 VDC with at least 1A. Some poor quality adaptors do not supply enough current as its marked rating. Try use a 12VDC adaptor with 1.5A or more. If the problem persists, return the device to its factory setting by pressing the reset button for five seconds until the device restarts.

- My GHTER-XX LCD screen suddenly freezes.

If you can connect to GHTER-XX from your PC, access to the Web-based administration interface and select Advanced Setting -> System -> System Reboot. Otherwise, disconnect the power supply and then reconnect to restart the device.

- I forgot my administrator password.

Press the reset button at the back of GHTER-XX 3 times to reset your system configuration settings back to factory default settings. The IP address will be restored to 192.168.1.100, the administrator username to admin, and the administrator password to abcd1234. Note that all face-prints and system log will be remained intact.

- I am having problem connecting my GHTER-XX to the network.

If you have two or more devices sharing the same network environment, make sure your GHTER-XX has a unique IP address. The factory default IP address is 192.168.1.100. You can set the IP address to any desired value by following the instructions in Chapter 3.

- My GHTER-XX is having problem capturing my face-print.

Make sure you position your face such that the FPGI face and eye frames turn yellow. It may be necessary to gently move your face forward and backward and nod your head up and down. In case of enrollment, you may decrease the quality check level to increase the speed of face print capture. In case of 1:N identification, note that the speed of recognition may take longer if you have a large library of enrolled users (more face-prints to compare).

6.1.1 • *How do I keep my firmware up to date?*

Your installer can update your firmware via the Internet by following the instructions in Chapter 3.

6.1.2 • *Where can I find my GHTER-XX product serial number?*

You can find your product serial number by looking under Basic -> Status menu on the web based administration interface. Or, you can find the same serial number at the sticker attached on the bottom of GHTER-XX Terminal.

6.1.3 • *What about service and support?*

GHTER-XX does not have any user-serviceable or replaceable parts. Always contact ARAS Security or our authorized service provider in case of physical damage. He can find online service and support information at the download section of the ARAS Security website (www.ARAS.nl).

7 Last But Not Least

For your safety and that of your equipments, please follow the instructions outlined in this chapter when handling and cleaning your TC-FACE©. Keep these instructions handy for reference.

Important Notes

Failure to follow the safety instruction could result in fire, electric shock, and other injury or damage.

7.1 Safety in Using and Handling GHTER-XX

Please follow these guidelines when using GHTER-XX .

- Do not attempt to open your GHTER-XX for any reason and under any condition as it does not contain any user-serviceable or replaceable parts. Furthermore, you run the risk of electric shock and voiding the limited warranty.
- Set up your GHTER-XX on a stable work environment that allows for adequate air circulation around the device. Do not operate your GHTER-XX on a soft surface as this can block the ventilation openings. Never insert objects into the ventilation openings.
- Keep your GHTER-XX away from moisture.
- Make sure the connector matches the port with the right orientation. Never force a connector into the port. If the connector and port do not join with reasonable ease, they probably do not match.
- Only use a power adaptor that outputs 12 VDC and up to 2 A for your GHTER-XX . As the power adaptor may become warm during normal use, always put the adaptor on a well ventilated area. Disconnect the power adaptor and another other cables if any of the following conditions exist.
 - o You wish to clean your GHTER-XX .
 - o The power adaptor becomes frayed or damaged.
 - o Your GHTER-XX or its power adaptor is exposed to excessive moisture.
 - o Your GHTER-XX has a damaged case, or you suspect physical damage.
- Use a damp, soft, lint-free cloth to clean your GHTER-XX exterior. Avoid getting moisture into any openings. Do not spray liquid directly onto your GHTER-XX . Do not use sprays, solvents, or abrasives that may damage the surface finish of your GHTER-XX .

7.2 FCC Regulatory Compliance Information

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance

with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment under FCC rules.

8 Appendix

8.1 Product Specifications

| | |
|-------------------------------|---|
| Imaging | |
| Camera | Hi-resolution CCD camera |
| Night vision | 22 build-in IR LED |
| Facial Recognition | |
| Technology | Near IR facial recognition |
| FAR | <0.001% |
| FRR | <0.5% |
| User capacity | 1000 users |
| Log capacity | 10,000 log events |
| User Interface | |
| Visual | 3.5 in TFT LCD |
| Audio | Alarm and alert buzzer |
| I/O Connectors | |
| Network | RJ-45 x 1 |
| Digital output | Relay x 2 |
| Digital input | Door sensor x 1; Exit switch x 1 |
| Wiegand interface | Input x 1; Output x 1 |
| Serial interface | RS-232, RS-485 |
| Power and Physical Dimensions | |
| Power supply | 12 VDC, 1 A |
| Dimension & weight | 80 cm x 88 cm x 175 cm, 800 gm |
| Network | |
| Ethernet | 10/100 Base-T |
| Protocol | TCP-IP, HTTP |
| Management & Support | |
| Administration | Web-based Administration Interface; EFR-API Software Development Kit |

8.2 Acronym List

| | |
|------|---|
| BIOS | Basic Input-Output System |
| CAT | Category |
| CCD | Charge-Coupled Device |
| COM | Common |
| DHCP | Dynamic Host Configuration Protocol |
| DIP | Dual In-line Package |
| DNS | Domain Name System |
| EMC | Electromagnetic Compliance |
| FAR | False Acceptance Rate |
| FAQ | Frequently Asked Question |
| FCC | Federal Communications Commission |
| FPGI | Facial Positioning Guidance Interface |
| FRR | False Rejection Rate |
| GND | Ground |
| HTTP | Hypertext Transfer Protocol |
| ID | Identification |
| IEEE | Institute of Electrical and Electronics Engineers |
| I/F | Interface |
| I/O | Input/Output |
| IP | Internet Protocol |
| IR | Infra-Red |
| LAN | Local Area Network |
| LCD | Liquid Crystal Display |
| LED | Light Emitting Diode |
| MCU | Microcontroller Unit |
| N.C. | Normal Close |
| NIC | Network Interface Controller |
| N.O. | Normal Open |
| OSD | On-Screen Display |
| PC | Personal Computer |
| RTC | Real-Time Clock |
| TCP | Transmission Control Protocol |
| TFT | Thin Film Transistor |
| VAC | Voltage Alternating Current |
| VDC | Voltage Direct Current |

8.3 Factory Default Configuration Settings

| Facial Recognition | |
|---------------------------|-----------------------|
| Operating mode | 1 to N identification |
| Recognition threshold | 85 |
| Network | |
| DHCP function | Disabled |
| Static IP address | 192.168.1.100 |
| Static IP netmask | 255.255.255.0 |
| Static IP gateway | 192.168.1.1 |
| DNS address | 168.95.1.1 |
| Web port | 80 |
| Firewall level | Low |
| Host name | EFR |
| I/O Control | |
| Door sensor alarm | Disabled |
| Door sensor polarity | Normal |
| Door sensor alarm time | 30 |
| Exit switch | Enabled |
| Relay #1 | Enabled |
| Relay #1 delay time | 0 |
| Relay #1 open time | 5 |
| Relay #2 | Enabled |
| Relay #2 delay time | 0 |
| Relay #2 open time | 5 |
| Wiegand | |
| Wiegand input | Enabled |
| Wiegand input facility ID | 0 |
| Wiegand input format | Standard 26-Bit |
| Wiegand output | Enabled |
| Wiegand output format | Standard 26-Bit |
| Display | |
| Draw face marker | Enabled |
| Log Configuration | |
| User enrolled | Log Message and Image |
| Authentication passed | Log Message and Image |
| Authentication denied | Log Message and Image |
| User registered | Log Disabled |
| User removed | Log Disabled |
| Unknown card ID | Log Message |

| | |
|-----------------------------|--------------|
| Door sensor triggered | Log Disabled |
| Exit switch triggered | Log Message |
| Tamper alarm | Log Message |
| Log-in passed | Log Disabled |
| Log-in denied | Log Message |
| Configuration changed | Log Message |
| Firmware updated | Log Message |
| EFR-API connected | Log Disabled |
| System boot-up | Log Message |
| Exiting sleep mode | Log Disabled |
| Password | |
| Admin username | admin |
| Admin password | psp1234 |
| User 1 username | user1 |
| User 2 username | user2 |
| User 3 username | user3 |
| System | |
| Power saving time | 10 second |
| Motion detector sensitivity | 5 |
| Language | English |