LM Series

User's Guide

iGuard®

Federal Communications Commission (FCC) Statement

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 in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

Reorient or relocate the receiving antenna.
Increase the separation between the equipment and receiver.
Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
Consult the dealer or an experienced radio/TV technician for help.

CE

EMC DIRECTIVE 89/336/EEC (EN55022 / EN55024)

Trade Name: iGuard
Model No: LM530

User's Notice

This manual contains detailed instructions and notes on the operation and use of the product. For your safety and benefit, read this manual carefully before using the product. Keep this manual in a handy place for quick reference.

Notes

- Some illustrations in this manual might be slightly different from the product.
- Certain options might not be available in some countries. For details, please contact your local dealer.

Important

Contents of this manual are subject to change without prior notice. In no event will the company be liable for direct, indirect, special, incidental, or consequential damages as a result of handling or operating the product.

Trademarks

- iGuard® is registered trademark of Lucky Technology Ltd.
- Microsoft® and Windows® are registered trademarks of Microsoft Corporation.
- Other product names used herein are for identification purposes only and might be trademarks of their respective companies. We disclaim any and all rights to those marks.

Table of Content

INSTALLATION

Proper planning is the key to successful implementation of any technology project. While the iGuard system is very easy to install and operate, there are some areas to consider before you begin installation.

Pre-Installation Notes

- iGuard is designed for indoor use. If you plan to install it outdoors, be aware that exposing it to water, heat, or other harsh conditions can damage the device and it may not operate properly.

- Do not install iGuard next to heat sources or in direct sunlight.

- To prevent electrical short-circuits or overload, power the iGuard independently with the power supply provided. Do not share the power with other device such as the electric door strike.

- To increase the security level in access control applications, use the optional *Remote Relay* together with the iGuard unit. This device is sold separately, and it assures that malicious damage to or tampering with the iGuard does not result in a release of the electric door strike. Please refer to the Appendix for more information.

- Make sure the *Smartcard Company Code* is properly set ***before*** assigning any smartcard to users. This code is a configurable, 4-character code, which is to set your iGuard system apart from any other iGuard system. Any smartcard with a code that does not match is not recognized by the system. So once the smartcards have been assigned, do not change this Company Code. Please refer to the section "*Using the Web Browser → System Setting → Device Setup → Basic → Company Code"* (page 50) for more information.

Installation

Determine the location(s) for installing iGuard, external *Remote Relay*, door strike and power supply line. Fasten the rear metal panel at the location where the iGuard unit will be installed. Connect the iGuard unit with the power supply provided.

Power Requirements & Back EMF issue

iGuard requires DC 12V / 800mA switching power supply. Sharing power with other devices, such as a door strike, is NOT recommended. This is because the potential back EMF (Electromotive Force) generated by the door strike may affect the iGuard. If it is necessary to share it with the door strike, a protection diode (1N4004 type) must be installed across the 12V power lines to the iGuard. Refer to the Connection Diagram in the Appendix for more information.

Warning: Use ONLY the power supply provided. Do not use other power supplies since this may lead to system failure, and poor or unreliable operation.

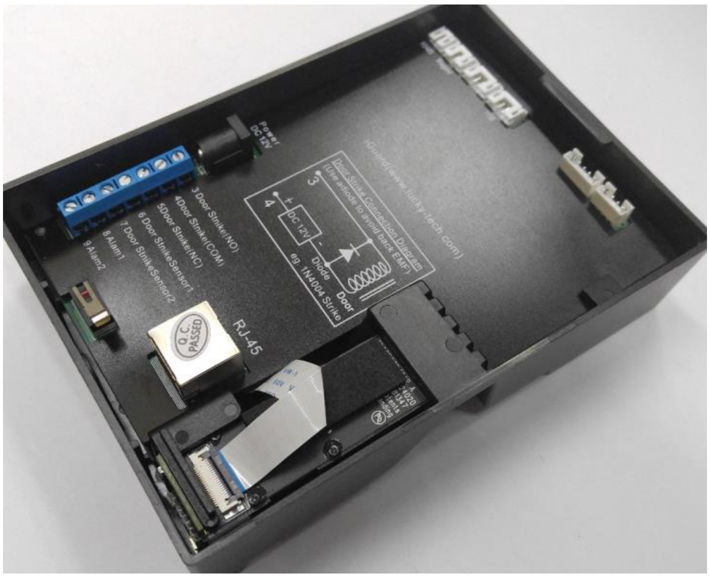
When deciding where to install…

iGuard is a wall-mounted unit with a miniscule footprint, and can be conveniently installed anywhere. However, for **access control** applications, it is recommended that the iGuard should be installed as close to the door as possible, so that the user can open the door within the timeout period, which is 5 seconds by default. Also note the following points:

- Make sure that air can circulate freely through the ventilation slots.
- Do not install the product next to heat-emitting sources, or in a place subject to direct sunlight and excessive dust.

Connect the Power & External Controls

iGuard provides easy-access terminals for connections to external controls, including Door Strikes, Door Sensor and External Alarm.



Terminals	Description
Power	**Power (12V DC)** The power requirement is 12V DC, 800mA. Connect it to the power supply provided.

Terminals	Description
3, 4 & 5	**Door Strike** Terminal #3 & #4 are the normal-open (NO) pair, and terminal #4 & #5 are the normal-close (NC) pair. Connect the door strike to either pair of these terminals according to the type of the electric door strike.
6 & 7	**Door Sensor (Optional)** This pair provides iGuard the current status of the door (i.e., open / close). If the door is left open for over 10 seconds, iGuard will generate beep sounds to alarm.
8 & 9	**External Alarm (Optional)** This pair is for the optional external alarm. In the case that the device is forced open and removed from the wall during operation, an internal case switch will connect this terminal pair, which can optionally sound an external alarm.
RS - 485 (for Remote Relay only)	**Remote Relay Connector** This is to connect the iGuard to the optional *Remote Door Relay* unit. Refer to the Appendix (p. 67) for more detail.
Wiegand	**Wiegand Connector** iGuard can be used as a Wiegand Reader. This Wiegand connector outputs the user ID to another Wiegand device in the standard 26-bit format.

Remarks: Terminals / Connectors other than the above mentioned are reserved for manufacturer use.

Connect the Electric Door Strike

Connect the Electric Door Strike to the Terminal Pair **#3 & #4** for normal-open type, or the pair **#4 & #5** for normal-close type.

Internally, these terminals #3, #4 & #5 are connected directly to an internal relay, rating at 12V / 1Amp. If the door strike is within this current limit, it can be directly connected to these terminals. If the current rating is above 1 Amp, a **Remote Door Relay** (sold separately) must be used (see Appendix on page 67).

More details about the door strike connection are given in the connection diagrams in the Appendix.

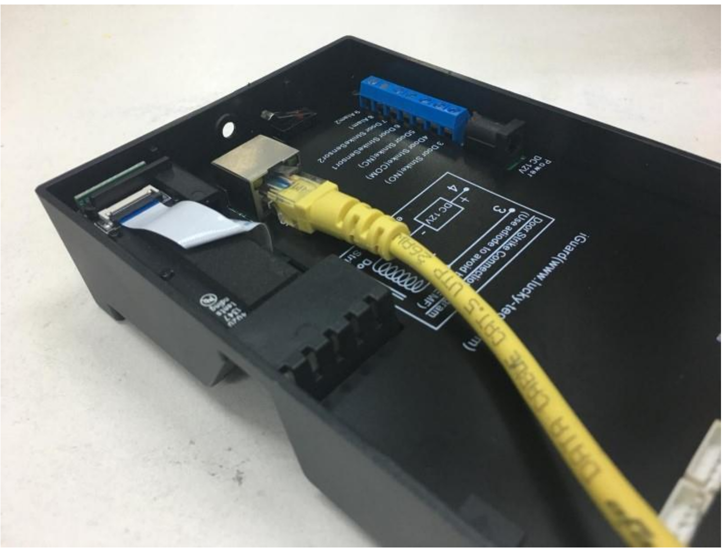
The administrator should examine each door that is to be controlled, and determine the type of door (wood, glass, or metal), the swing direction, the desired in/out direction to be controlled (unless the unit will authenticate both directions), and the type of frame (wood or metal). This information will be helpful for determining the type of lock that is to be used with the iGuard. Please consult the dealer for more information about magnetic locks, electric strikes, and other door hardware.

If the system is used solely for Time Attendance purposes, these terminals can be left disconnected.

Connect the Network

iGuard is designed to be directly connected to the corporate computer network and to the Internet via the standard RJ-45 cabling. By connecting it to the network, one can manage & monitor the unit via any standard web browser, such as Microsoft Edge & Google Chrome.

The connection is very straightforward as shown in the following picture:



Make sure the computer has installed and has been configured with the TCP/IP Protocols.

iGuard can also be connected directly to the PC via crossover RJ-45 cable.

Note: Please contact iGuard Technical Support at info@lucky.com.hk for technical support.

Power-up

During power up, iGuard will perform a self-test, then it will enter the standby mode as shown below: -

Description	***LCD Display***
1. Power Up – when iGuard is powering-up, it will perform a self-test…	`Initializing...`

Description ***LCD Display***

2. After about 10 sec., the device will load the system program…

```
iGuard System
Loading.....
```

3. After loading the system program, iGuard will enter the Standby Mode and is now ready to set the date, time & the network settings.

```
Wed Jan 24 12:00
ID #:_        IN
```

CONFIGURATION

Setting the date and time

The date and time must be properly set up so that iGuard can time stamp all the access & time attendance records. **iGuard automatically sync its clock with the SNTP Time Server in the internet.** It can also be done manually as follow:

Description ***LCD Display***

1. While in Standby Mode, press the **Func** key to enter the Function Menu. You will be asked to enter the System Administrator Password.

```
Enter Password:
_
```

2. Enter the System Administrator Password (default: 123).

```
Enter Password:
***_
```

3. Press the **Func** key to continue. The function menu will scroll down slowly as shown.

```
Press 1:
Add/Update ID
```

:

```
Press 5: System
Configuration...
```

4. Enter **5** to select the **System Configuration** menu. The current firmware version & the IP address will be momentarily shown, followed by the current date. If necessary, enter the new date and then press the **Func** key to continue.

```
Ver: 6.0.1008
192.168.000.100
```

:

```
Date (M/D/Y):
01/24/2018
```

5. After pressing the **Func** key, the current time is displayed. Enter the new time then press the **Func** key to continue.

```
Time (H:M:S):
13:24:43
```

6. The system will then ask for the Terminal ID, which is used to identify the iGuard in your network. The default ID is “iGuard”. This ID is important especially if you have more than one unit installed.

```
Terminal ID:
iGuard
```

Note: iGuard can keep the date & time running without power for approximately one day.

Network Settings

To connect iGuard directly to your corporate network, a device name & an IP address are required. It is optional to use the DHCP server in the network to dynamically assign the IP address, but it is suggested that a static IP address is to be used.

The following procedures describe how to assign the name (i.e., the Terminal ID), the IP addresses, and other related network settings. Before proceeding the correct settings should already be obtained from the network administrator.

Description ***LCD Display***

1. *(…continue from step 6 above)* Enter the name of the device (e.g., A142). A more meaningful & descriptive name, such as “front door” or “main entrance”, can be assigned through the setup pages of the Web Interface (discussed in next chapter).

```
Terminal ID:
A142_
```

2. Press **Func** key to continue, and then press **2** to select “Static IP” instead of DHCP for now.

```
DHCP/Static IP
(1/2)? Static
```

3. Press **Func** key to continue. You will then be asked to enter the IP address of the device. The default is 192.168.0.100. Change this default value if necessary.

```
IP Address:
192.168.000.100
```

4. Press **Func** key, and then you will be asked to enter the port number. Use the default value 80 for now.

```
Port Number:
80_
```

5. Press **Func** key to continue. Enter the subnet mask here (e.g., 255.255.255.0).

```
SubnetMask:
255.255.255.000
```

6. Press **Func** key to continue. Enter the address of the Default Gateway (e.g., 192.168.0.1).

```
Default Gateway:
192.168.000.001
```

7. Press **Func** key to continue. Enter the address of the Domain Name Server (e.g., 1.1.1.1).

```
DNS:
001.001.001.001
```

8. Press **Func** key to continue. You will be asked if the device is a *Master* or *Slave* device. This is useful in a multi-device environment, where more than one iGuard are connected to each other. Refer to the section “*Master & Slave Mode*” for more detail.

```
Master/Slave:
(1/2)? Master
```

9. Press **1** to select *Master* for now. You will be asked if the device is connecting to **iGuardPayroll** or not. **iGuardPayroll** is a free service to allow you to store user’s data and access logs in our cloud server. Refer to the appendix for more detail.

```
Use iGuardPayrol
(Yes/No) 1/2? Y
```

:

```
iGuardPayroll...
(Yes/No)? Y
```

Description **LCD Display**

10. Press **2** to disable iGuardPayroll for now. When asked if you would accept the changes, press **1** to select `Yes`. The system may then reset itself and return to Standby Mode.

```
OK to Accept Y/N
(1/2)? Yes
```

:

```
Wed Jan 24 12:01
ID #:_        IN
```

Warning: The IP address of the iGuard unit must be unique as in all other network devices. Otherwise, it will cause a network error and the iGuard will not function properly.

Note: The Terminal ID is NOT required to be unique, but a unique ID is recommended if multiple devices are installed in the same computer network, such as in a *Master / Slave* configuration.

Verifying the Network Connections

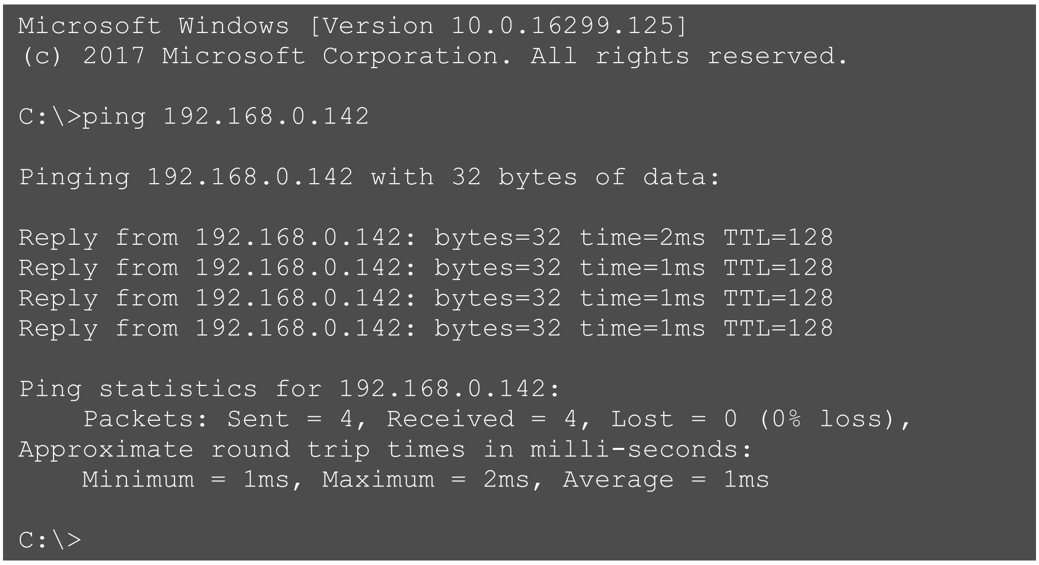
One can test the above network settings by using a PC to *ping* the iGuard unit as follows:-

- Open the Command Prompt on the PC. To open Command Prompt for Windows machines, click **Start** and then type **cmd**, and then select Command Prompt.

- Type **ipconfig** to check the IP address of the PC and make sure it is in the same network as iGuard (i.e., the same subnet mask).

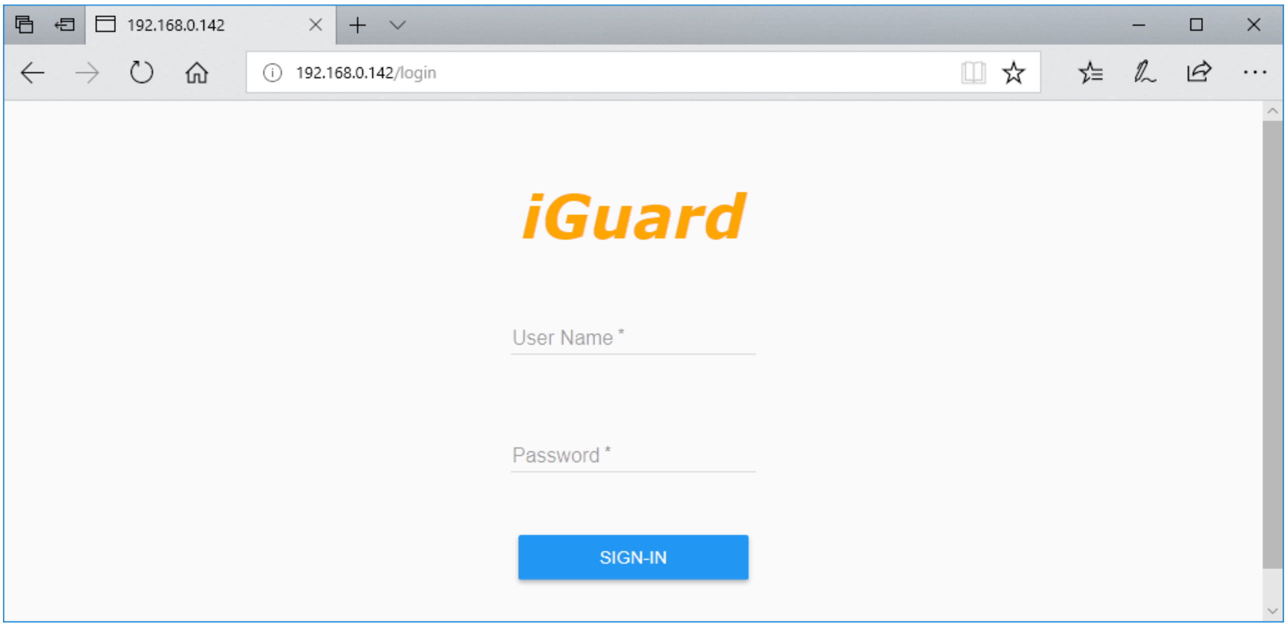
- While still in the Command Prompt, use the **ping** command to ping the IP address of the iGuard unit as shown below, which is 192.168.0.142 in this case.

- If the ping responds the following, the IP is set properly and the unit is ready.

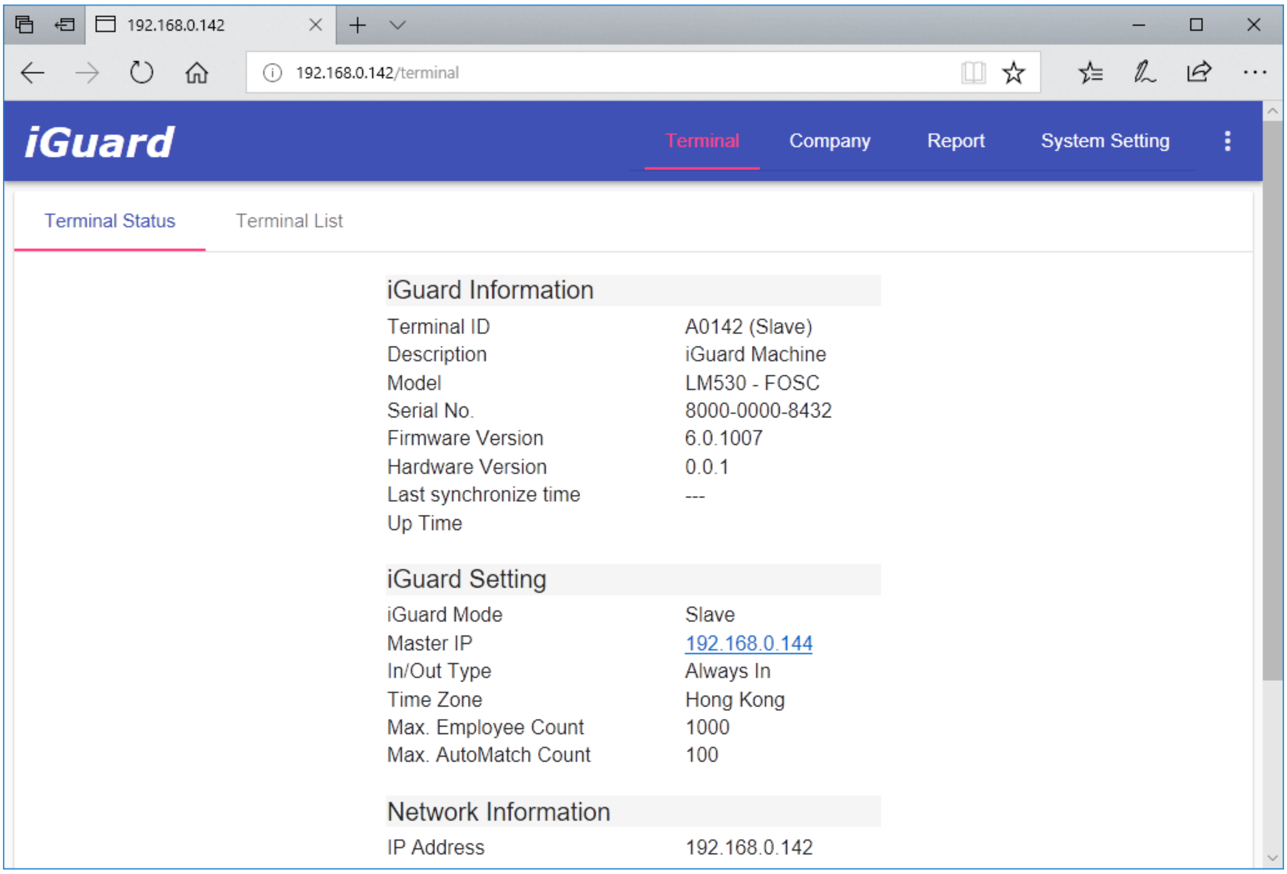


```
Microsoft Windows [Version 10.0.16299.125]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\>ping 192.168.0.142

Pinging 192.168.0.142 with 32 bytes of data:

Reply from 192.168.0.142: bytes=32 time=2ms TTL=128
Reply from 192.168.0.142: bytes=32 time=1ms TTL=128
Reply from 192.168.0.142: bytes=32 time=1ms TTL=128
Reply from 192.168.0.142: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.0.142:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 2ms, Average = 1ms

C:\>
```

Next, launch the PC web browser (e.g., Microsoft Edge or Google Chrome), and enter the IP address **http://192.168.0.142** (i.e., the IP Address of the iGuard), and the following iGuard web interface will be shown in the browser window:-



Enter the default user name and password (admin / 123), and the following screen will appear:-



iGuard Information

Terminal ID	A0142 (Slave)
Description	iGuard Machine
Model	LM530 - FOSC
Serial No.	8000-0000-8432
Firmware Version	6.0.1007
Hardware Version	0.0.1
Last synchronize time	---
Up Time	

iGuard Setting

iGuard Mode	Slave
Master IP	192.168.0.144
In/Out Type	Always In
Time Zone	Hong Kong
Max. Employee Count	1000
Max. AutoMatch Count	100

Network Information

IP Address	192.168.0.142

At this stage, the basic configuration is complete, and iGuard is now ready to use.

Getting Started

iGuard is a self-contained, platform independent access control and time attendance device. Most of the basic operations, such as user registration and verification, can be directly performed using the keypad of the unit itself without using the computer and the web browser.

Other operations like connecting and configuring Master/Slave devices and issuing smartcard, can also be done through the keypad.

More advanced features, such as setting the users' access rights, retrieving the access log and other reports, and connecting to the cloud service, require accessing the device via the built-in web server through a web browser (e.g., Microsoft Edge or Google Chrome).

User Authentication

There are three methods for user authentication. These are the *Contactless Smartcard*, the *Fingerprint* (for model LM530-FOSC only) and the *Personal Password*. Each of these methods can be used separately to authenticate a user.

Alternatively, smartcard and fingerprint / personal password can be combined together during user authentication to achieve higher security level of verification.

This section discusses the basic operations of these three methods.

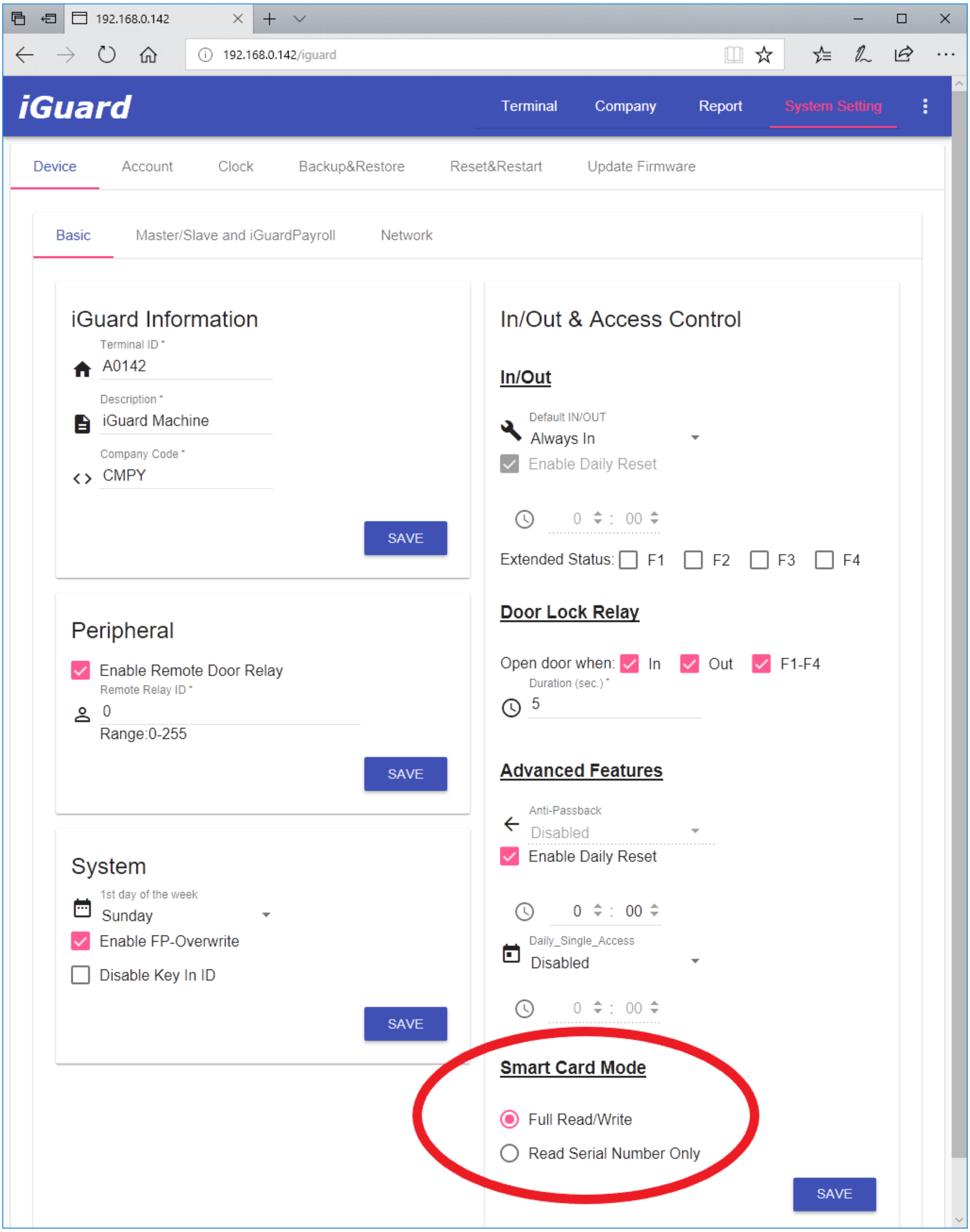
SmartCard

iGuard comes standard with built-in contactless smartcard reader. The System Administrator can use smartcard to create a new user, or to assign a smartcard to an existing user.

Smartcard allows almost-instant verification for users, and it comes in handy when the device is used during the high-traffic period, for example, at the beginning of the day when everyone gets to the office at around the same time.

Alternatively, for iGuard model with fingerprint sensor (LM530-FOSC), fingerprint verification can also be done together with smartcard, to increase the verification's security level. In this case, after presenting the smartcard, the user will be asked to scan his fingerprint for authentication.

iGuard operates in two smartcard modes: *Full Read-Write* mode and *Serial-Number-Only* mode. It can be set with the built-in webpage at **System Setting → Device → Basic → SmartCard Mode**, as shown in the following screen:



iGuard Information

Terminal ID *: A0142

Description *: iGuard Machine

Company Code *: CMPY

Peripheral

☑ Enable Remote Door Relay

Remote Relay ID *: 0

Range:0-255

System

1st day of the week: Sunday

☑ Enable FP-Overwrite

☐ Disable Key In ID

In/Out & Access Control

In/Out

Default IN/OUT: Always In

☑ Enable Daily Reset

0 : 00

Extended Status: ☐ F1 ☐ F2 ☐ F3 ☐ F4

Door Lock Relay

Open door when: ☑ In ☑ Out ☑ F1-F4

Duration (sec.) *: 5

Advanced Features

Anti-Passback: Disabled

☑ Enable Daily Reset

0 : 00

Daily_Single_Access: Disabled

0 : 00

Smart Card Mode

● Full Read/Write

○ Read Serial Number Only

Full Read / Write Mode

In the Full-Read-Write mode, for each individual user, all the available user information including the user name, personal password, access rights, and the fingerprint information (if any), will be written to the Smartcard’s internal memory.

Under this mode, administers can choose saving the users' fingerprint information in both the iGuard device and the smartcards at the same time, or just saving it to smartcards only.

For privacy purpose, one can choose to save his fingerprint information to the smartcard only.

The operation of writing data to smartcards involves accessing the internal memory of the smartcards with special smartcard password and access rights, therefore, for security reason, only specifically-formatted iGuard Smartcard (sold separately) can be used in this mode.

Please contact the iGuard dealer or visit the manufacturer's website[1] for more information about purchasing the smartcards for this mode of operation.

Serial Number Only Mode

In the Serial-Number-Only mode, iGuard only reads the serial number of the smartcard. The content of the smartcard content is ignored. The smartcard serial number is used to identify each individual user. The user information is retrieved from iGuard's internal database rather than read from the smartcard for further verification and authentication.

Smartcards Supported by iGuard

Each mode supports different kinds of smartcards as follows:

ISO	Type	Full Read / Write	S/N Only
ISO14443A	Mifare Classic	✓	✓
	Mifare Classic 4K	✓	✓
	Mifare Plus	✗	✓
	Mifare Mini	✗	✓
	Mifare Desfire / Desfire-EV1	✗	✓
	Siemens Infineon	✓	✓
ISO18092	Sony Felica [2] e.g., the HK's Octopus Card	✗	✓

Note: In the *Full-Read-Write* mode, only specifically-formatted iGuard Smartcard can be used with the device. Please contact the iGuard dealer or visit the manufacturer's website for more information about purchasing the Smartcard.

[1] http://www.lucky-tech.com

[2] The Octopus Card commonly used in Hong Kong also uses this standard.

Adding New User with Smartcard

Follow these steps to create a new user by issuing a new smartcard to the user:-

Description	***LCD Display***

1. While in Standby Mode, press the **Func** key to enter the Function Menu. Enter the System Administrator Password (default 123) and press **Func** key, then press **9** to select the item "Issue / Import Smartcard".	`Issue/Import`
	`Card (1/2)? _`

2. Enter **1** to select "Issue Card". You will then be asked to enter the User ID.	`Enter ID #`
	`_`

3. Enter the user ID # (e.g. A01). The ID can be of any length from 1 to 10 characters, including the letters A & B.	`Enter ID #`
	`A01_`

4. Press **Func** key to continue. If the ID does not exist, you will be asked to confirm to create this new ID.	`Create new ID...`
	`Yes/No (1/2)? _`

5. Press **1** to select **Yes**, then the unit will prompt you to present the Smartcard.	`Waiting for`
	`SmartCard...`

6. Place a new Smartcard near the Keypad. Depending on the selected smartcard mode, once the device has detected the Smartcard, it will either update the card by writing the user information to the card, or just assign the smartcard's serial number to the user.	`Writing...`
	:
	`Issue OK!`

7. Once it has finished updating the card, the unit will ask for the next user ID for issuing another Smartcard. Press **backspace** to return to Standby Mode.	`Thu Aug 30 13:28`
	`ID #:_         IN`

In **Full-Read-Write mode**, all the available user information, including the user name, personal password, access rights, and the fingerprint information (if any), will be written to the Smartcard memory.

In **Serial-Number-Only mode**, iGuard will only read the serial number of the smartcard, and assign this serial number to the user, without writing any user information to the smartcard.

Verification with Smartcard

Verification with Smartcard is simple and straight forward, and is illustrated in the following steps:-

Description	***LCD Display***
1. While in Standby Mode, present the smart card near the keypad. Depending on the card type, the unit will either read the card's s/n only or read the whole content of the card. If the card is valid, the user will be authorized as indicated in the display. The unit will return to Standby Mode afterwards, and it is ready for the next card.	**A01** **Authorized!** **:** **Thu Aug 30 13:36** **ID #:_ IN**

Note: To achieve higher security level, iGuard can be configured to ask for the ***fingerprint image*** or ***Personal Password*** after presenting the smartcard for verification. It will be discussed in more detail in the next section under the heading "*Function 9: Issue / Import Card*".

Adding & Verifying user with Fingerprint (for LM530-FOSC only)

(This section is for iGuard with the optional fingerprint sensor only)

iGuard is optionally equipped with fingerprint sensor for fingerprint verification.

During the fingerprint enrollment process, the unit will ask for two fingerprint images for each person, and the information of the images (i.e., minutiae[3]) is extracted and stored in the internal database for later verification.

Each person must register two fingers: one as the primary and the other one as the secondary. Therefore, if the person's primary finger is temporarily not suitable, such as when the finger is wounded, he can still use his secondary finger for verification.

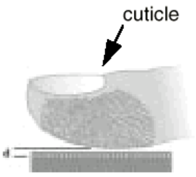
During the process, each fingerprint image is captured two times for minutiae analysis and extraction. If the quality of any one of these two images is not good enough, the user will be asked to re-scan the two images again.

The two thumbs are suggested as the primary & secondary fingers. This is because the thumbs are usually bigger and can cover the scanner area better.

Hints for Capturing Fingerprint Images

Place the thumb flat on the fingerprint sensor using the pad, not the tip, of the thumb. The tip of the thumb contains the fewest minutia points, so place the thumb as flat as possible on the sensor to generate the fullest possible image.

[3] Minutiae is the mathematical representation of the fingerprint image. It cannot be used to revert the original fingerprint image.



The Core

The Tip

The core of the fingerprint containing the most minutia points is usually located opposite the cuticle.   Center the cuticle in the sensor window to maximize the number of minutia points.

IMPORTANT: During the enrollment process, position the center of the fingerprint of the thumb to the center of the fingerprint sensor. The center of the fingerprint contains the most minutia points from which the fingerprint sensor can extract. *A good fingerprint image captured during the enrollment process can significantly reduce the false-reject rate during later verification.*

Adding New User with Fingerprint

The following steps will show how to register the user's fingerprint data:-

Description	***LCD Display***
1. While in Standby Mode, press the **Func** key to enter the Function Menu. Enter the System Administrator Password (default 123) and press **Func** key, then press **1** to select "**Add/Update ID**" menu.	**By Finger/Passwd** **(1/2)? _**
2. Press **1** to select "By Finger", then you will be asked to enter the user ID.	**Enter ID #:** **_**
3. Enter the user ID # (e.g. **A02**). The ID can be of any length from 1 to 10 characters.	**Enter ID #:** **A02_**
4. Press the **Func** key to confirm the ID #. You will be asked to place the finger on the fingerprint scanner.	**Scanning 1/2** **Waiting finger..**
5. Place the primary finger on the scanner for scanning. Afterwards, you will be asked to scan this same finger again.	**Press Func to** **scan 2 of 2...**
6. Remove the finger from the scanner and then press **Func**. Then scan the *same* finger again for the 2nd time. After that, iGuard will analyze and extract the data from the two images. If the image quality is good, it will then ask for the secondary finger. Otherwise, it will ask to scan the 1st finger again.	**Analyzing...** : **Analyzing...OK** : **Press Func to** **scan 2nd Finger**

Description **LCD Display**

7. Press **Func**, then repeat the procedure for the secondary finger. After successfully scanning the 2nd finger, iGuard will ask if the AutoMatch[4] feature is to be enabled for this user.

```
Add to AutoMatch
Yes/No (1/2)?_
```

8. Press **1** to enable this feature for this user. iGuard will then update the internal database and the fingerprint sensor, and prompt for more users.

```

Updating...
```

:

```
ID# A02
Added OK!
```

:

```
Enter ID#:
_
```

9. Press the **Backspace** to return to the Standby mode.

```
Thu Aug 30 13:34
ID #:_        IN
```

Note: If the user ID “A02” already exists, iGuard will prompt and ask whether to overwrite the existing fingerprint information or not.

In case of poor fingerprint image, for example, if the skin of a user is too dry or too wet, the user might experience difficulty when registering the fingerprint image. In this case, iGuard will show related messages indicating the fingerprint quality problem.

Please refer to the *Fingerprint Enrollment* section in the Appendix for more information.

Verification

iGuard uses the enrolled fingerprint information to identify the person. The verification process is very straightforward, and is illustrated in the following steps: -

Description **LCD Display**

1. While in Standby Mode, key in the user ID number (e.g., **A02**).

```
Thu Aug 30 13:36
A02_          IN
```

2. Place either one of the registered fingers on the fingerprint scanner. You should place the finger the same way that you did during the enrollment procedure. The device will automatically start scanning after detecting the presence of the finger.

```
Scanning...
A02_
```

:

```

Verifying...
```

[4] AutoMatch is a feature that allows users to get authenticated by simply placing the finger on the scanner, without first entering the user ID. The maximum number of AutoMatch Users is 100.

Description ***LCD Display***

3. If you are authenticated, the authorized message will be shown briefly, and the unit will return to the Standby Mode.

```

Authorized!
```

:

```
Thu Aug 30 13:36
ID #:_         IN
```

Note: If the AutoMatch feature is enabled for a user, this user can simply place her finger on the scanner for authentication without the need to enter her ID first. This feature is also called "1 to Many Matching", and it will be discussed in more detail in the "*Keypad Operation*" section.

Adding and Verifying user with Personal Password

In additional to Fingerprint and Smartcard, the user can also use the personal password for verification. The personal password is useful for the user who is not able (or is not willing) to use fingerprint for verification (such as having skin problems), and does not want to use Smartcard.

Adding User with Personal Password

The following steps demonstrate how to add a new user with personal password:-

Description ***LCD Display***

1. While in Standby Mode, press the **Func** key to enter the Function Menu. Enter the System Administrator Password (default 123) and press **Func** key, then press **1** to select "Add/Update ID" menu.

```
By Finger/Passwd
(1/2)? _
```

2. Press **2** to select "By Password", then you will be asked to enter the user ID.

```
Enter ID #:
_
```

3. Enter the ID (e.g., **A03**).

```
Enter ID #:
A03_
```

4. Press the **Func** to confirm. Then enter the Personal Password for user A03. The password length can be up to 8 characters, including the characters A & B (e.g. 1234AB).

```
User Password:
******_
```

5. Press **Func** to confirm. This new user has been added to the unit. The unit will then ask for the next ID to add.

```
ID: A03
Added OK!
```

:

```
Enter ID #:
_
```

Description	***LCD Display***
6. Press **Backspace** to return to Standby Mode.	**Thu Aug 30 13:34** **ID #:_ IN**

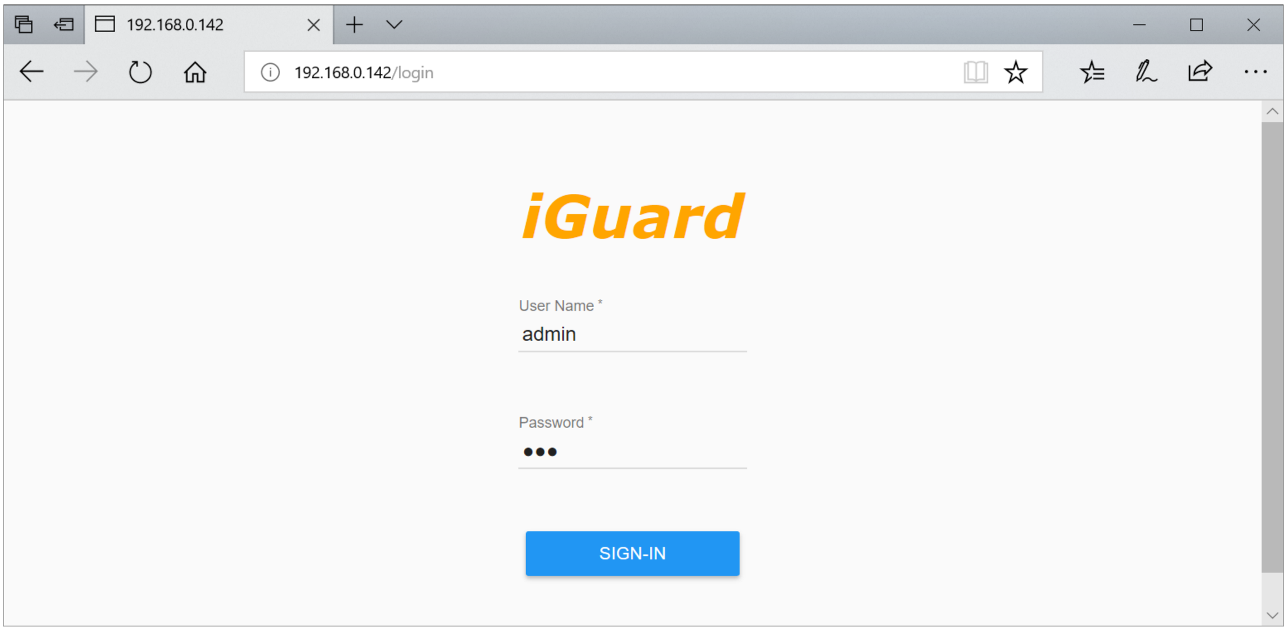
Verification with Personal Password

Once the personal password is assigned, the user can use it to get authenticated as follows:-

Description	***LCD Display***
1. While in Standby Mode, key in the user ID number (e.g., **A03**).	**Thu Aug 30 13:36** **A03_ IN**
2. Instead of using the fingerprint, press the **Func** key to indicate you are using the Personal Password. The unit will prompt you to enter the Personal Password.	**Your Password:** **_**
3. Enter the Personal Password (e.g., 1234AB).	**Your Password:** ********_**
4. Press the **Func** to confirm. If the password is correct, the unit will authorize the user, and will return to the Standby Mode as shown.	**A03** **Authorized!** **:** **Thu Aug 30 13:36** **ID #:_ IN**

Viewing the Access Log

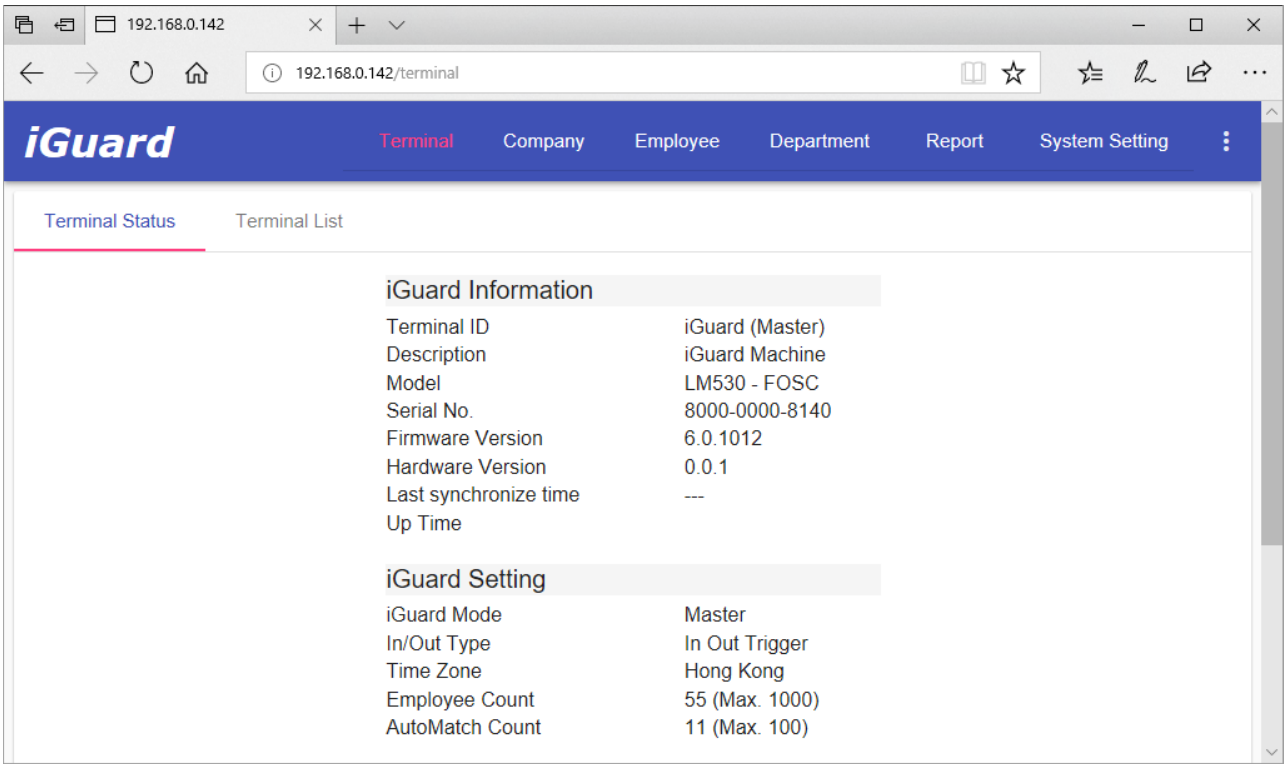
In the Web Browser, enter the IP address of the iGuard (e.g. http://192.168.0.142) to go to the iGuard webpage.



User Name *
admin

Password *
●●●

Enter the default user name and password (admin/123) to log in.



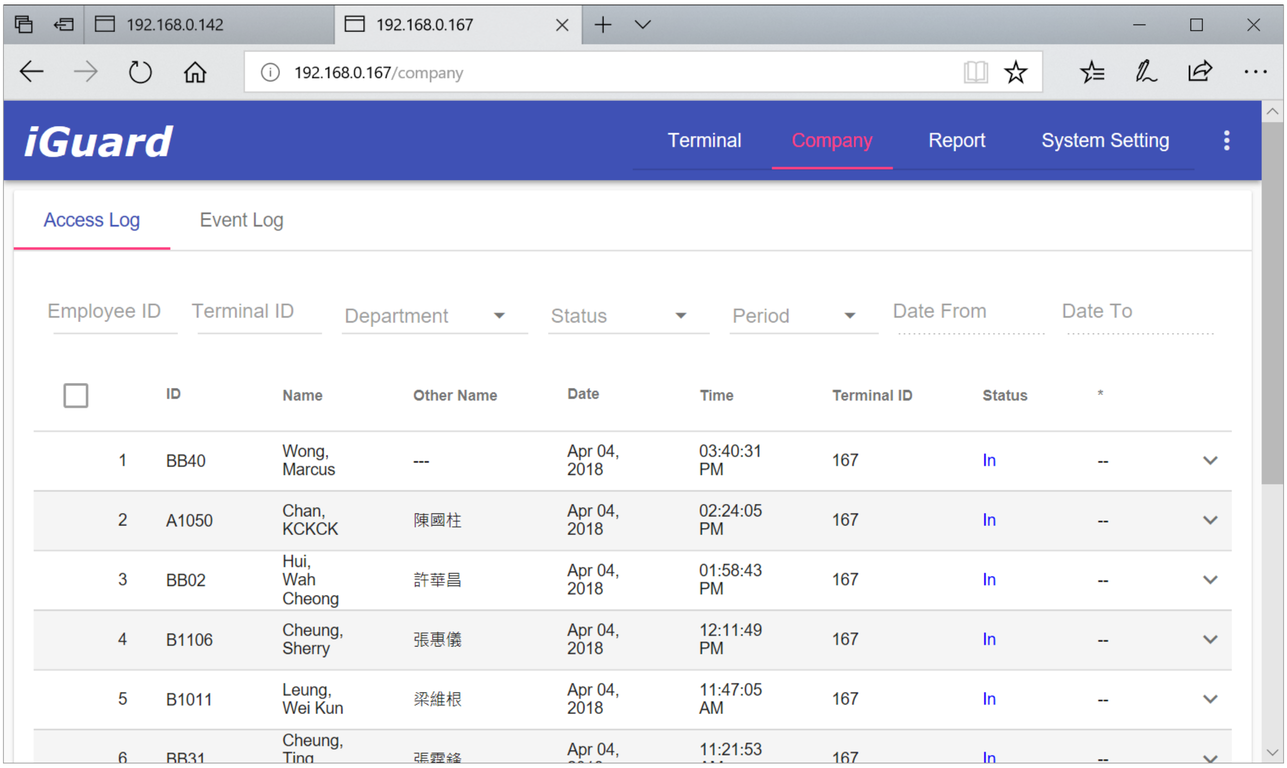
iGuard Information

Terminal ID	iGuard (Master)
Description	iGuard Machine
Model	LM530 - FOSC
Serial No.	8000-0000-8140
Firmware Version	6.0.1012
Hardware Version	0.0.1
Last synchronize time	---
Up Time	

iGuard Setting

iGuard Mode	Master
In/Out Type	In Out Trigger
Time Zone	Hong Kong
Employee Count	55 (Max. 1000)
AutoMatch Count	11 (Max. 100)

Select Company in the menu at the top will take you to the Access Log as follows:



□	ID	Name	Other Name	Date	Time	Terminal ID	Status	*
1	BB40	Wong, Marcus	---	Apr 04, 2018	03:40:31 PM	167	In	--
2	A1050	Chan, KCKCK	陳國柱	Apr 04, 2018	02:24:05 PM	167	In	--
3	BB02	Hui, Wah Cheong	許華昌	Apr 04, 2018	01:58:43 PM	167	In	--
4	B1106	Cheung, Sherry	張惠儀	Apr 04, 2018	12:11:49 PM	167	In	--
5	B1011	Leung, Wei Kun	梁維根	Apr 04, 2018	11:47:05 AM	167	In	--
6	BB31	Cheung, Ting	張霽峰	Apr 04,	11:21:53	167	In	--

Note: Additional functionality is available through the keypad operation and web interface, which will be discussed in coming chapters.

Master and Slave Mode

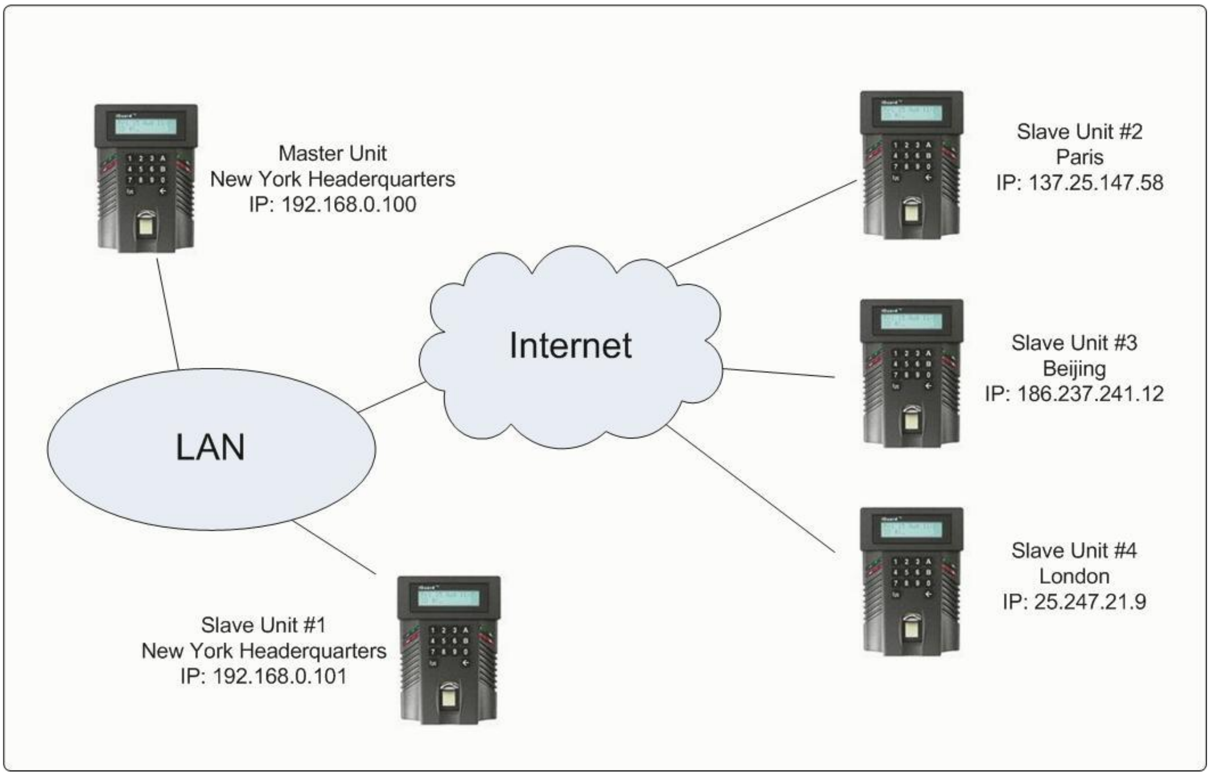
Each iGuard can be configured as a *Master* unit or a *Slave* unit.

By default, iGuard is configured as a Master unit. In a multi-device environment where more than one iGuard device is connected to the same corporate network or over the internet, these devices can form a Master / Slave network. In this case, one of these devices is assigned as the Master unit, and all others are assigned as Slave units.

The advantages of forming a Master / Slave network are:

- The system automatically replicates all the users' information to all devices in the master / slave network.
- Once a user has registered in a unit (***either*** a Master or a Slave unit), the information will become available in all units in the same network, and the user can get access to and verified by any one of the devices in the network.
- All access log records, such as the Clock-in and Clock-out records, created in any of these units are collectively saved in the Master unit, allowing the administrator to retrieve the access log records for all devices from a single location.
- Different access rights can be assigned to each individual iGuard unit.
- The master unit can optionally synchronize its clock with all the slave units (time zone adjusted).

The following is a typical Master / Slave setup:



In the above example, the Master unit is located in the New York Headquarters, and the other Slave units are installed in various places connected via the Internet. All the user information is available to all these units, and all the access log records of all these units are centrally saved in the Master unit.

How it works

The Master unit stores a completed set of user information in its internal database.

If a user is registered or modified in a Slave unit, this Slave unit will always replicate the new or updated information to the Master unit.

Whether or not the Master unit will replicate the information to all slaves depends on the type of information. If a particular user is an existing user and the user's information is modified, the Master will replicate the updated user information to all slaves immediately.

However, if it is a new user registered to the system, the Master unit will NOT replicate the information of the new user to the slave units in order to save the network bandwidth. It will only be saved in its internal database.

If the new user information is required by a particular Slave unit, the slave unit will send a request to the Master unit, and the Master unit will accordingly return the user information to that Slave unit. And similar to the Master unit, the Slave unit will then save the information in its internal database.

In other words, the Master unit only sends the new user information to others slaves on request.

Therefore, in case of network failure, a Slave unit will still be operational limited to the users who had previously been authenticated by the unit, since the unit already has these users' information stored in its internal database as a result of the previous requests to the Master unit.

Any new access log records will be updated to the Master unit automatically once the network connection is established again.

Basic Master / Slave configuration

The iGuard unit is configured as Master by default. Follow these steps to configure the unit as a Slave unit:-

Description	***LCD Display***

1. While in Standby Mode, press the **Func** key to enter the Function Menu. You will be prompted to enter the System Administrator Password as shown.	`Enter Password:`
	`_`

2. Enter the System Administrator Password (default: 123).	`Enter Password:`
	`***_`

3. Press the **Func** key to continue, and the function menu will appear.	`Press 1:`
	`Add/Update ID`

Description ***LCD Display***

4. Enter **5** to select the **System Configuration** menu. The firmware version and the IP address of the unit will appear briefly, and then the current date is displayed.

```
Ver: 6.0.1008
192.168.0.142
```

:

```
Date (M/D/Y):
01/24/2018
```

5. Press the **Func** key 9 times to skip the other settings. You will then see the message asking if this unit is a master or slave unit.

```
Master/Slave
(1/2)? Master
```

6. Then a scrolling message will appear to ask if it is to be connected to our cloud service and use the service as the Master unit. Enter **2** (No) for now.

```
Use iGuardPayrol
(Yes/No)1/2?_
```

:

scrolling message →

```
as Master... Use
1/2 (Yes/No)?_
```

7. Enter **2** to select *Slave*. Then the unit will ask for the IP address of the Master unit.

```
Master IP Addr:
192.168.000.100
```

8. Enter the IP address and press the **Func** key to continue. You will then be asked to enter the port number of the Master unit.

```
Master Port:
80_
```

9. Enter the port number and press the **Func** key. The unit will reboot itself and then return to the Standby Mode.

```
Thu Aug 30 13:25
ID #:_        IN
```

10. After a few seconds, if the Master unit can be reached, the user database will be synchronized from the master unit to this slave unit, and the corresponding message will appear during the process.

```
Synchronizing,
Please Wait...
```

11. Once the synchronization is done, the unit will return to standby mode, and is ready for use.

```
Thu Aug 30 13:28
ID #:_        IN
```

If the master unit is not reachable (e.g., the network connection is lost or the Master's IP address is wrong), the error message "*Master Offline!*" will appear on the LCD display.

Note: It is suggested that all units run on the same *firmware* version in a Master / Slave network. And one cannot mix the other iGuard model (e.g. the FPS model) with the LM model in a network.

Note: For security reason, the system administrator password of the slave unit must be the same as the Master unit. Otherwise, the master unit will reject the slave unit, and the error message "*Master Password Mismatch*" will appear.

Note: iGuard LM530 can work with the previous iGuard models, such as LM520, in forming a Master / Slave network, provided that:

- The previous model unit is configured as a Slave unit (i.e., the old unit cannot be the master unit of a LM530 unit), and
- The firmware version of the previous model unit is 5.0.9334 or later.

Currently iGuard does not support ***iGuardExpress***[5]. We do have plan to include ***iGuardExpress*** in the Master/Slave network described above in the future.

KEYPAD OPERATION

This section will discuss the **Func** Key (i.e. the Function Menu) and the **Backspace** Key. More functions and options are available in the built-in web interface, which will be discussed in the next section.

The Function menu

To enter the Function Menu, press the **Func** key in the Standby Mode and enter the System Administrator Password (default 123), then press the **Func** key again to confirm the password. Then the device will scroll and display all the available functions one by one.

There are 12 entries in the Function Menu, i.e., Function 0 to 9, A & B. They can be selected by pressing the corresponding key in the Function Menu.

The Function Menu	
Function 1 – Add / Update User	Function 7 – System Shutdown / Reset
Function 2 – Inactivate User	Function 8 – Set / Reset AutoMatch
Function 3 – Activate User	Function 9 – Issue / Import Smartcard
Function 4 – Delete User Fingerprint / ID	Function 0 – Advanced Feature
Function 5 – System Configuration	Function A – Toggle Test Mode
Function 6 – Set System Password	Function B – Open Door

Function 1: Add / Update User

This function is for adding a new user or updating an existing user by Fingerprint or Personal Password, as already discussed in the last section, *Getting Started*.

Function 2: Inactivate ID

A user ID can be temporarily suspended. This is useful if it is required to temporary remove a person's access to the facility, but might allow him to access again in the future.

[5] ***iGuardExpress*** is a Time-Attendance machine with built-in camera to take snap-shot of each clock-in / -out record. Please visit our website www.lucky-tech.com for more information.

This is done via the function "Inactivate ID" in the function menu, and it is illustrated in the following steps:-

Description	***LCD Display***
1. While in the Function Menu, press **2** to select *"Inactivate ID"* menu.	**Enter ID #:** **_**
2. Enter the ID # you want to suspend (e.g., A01).	**Enter ID #:** **A01_**
3. Press the **Func** key to confirm. The ID # is suspended, and the user can no longer be authenticated. Press **Backspace** to return to Standby mode.	**ID# A01** **Inactivated!** **:** **Thu Aug 30 13:44** **ID #:_ IN**

Function 3: Activate ID

This is to resume an Inactivated ID, and it follows the procedure similar to its counterpart function above.

Function 4: Delete Fingerprint / ID

Use this function to delete the fingerprint template of a user, or to permanently delete a user from the internal memory.

Follow these steps to delete the *fingerprint template* of the user:-

Description	***LCD Display***
1. While in the Function Menu, press **4** to select "Del Finger/ID".	**Del Finger/ID** **(1/2)? _**
2. Enter **1** to select Finger. Then you will be asked to enter the user ID that the fingerprint template is to be deleted.	**ID to Del Finger** **A01_**
3. Press the **Func** key to confirm. The Fingerprint Template of the user is deleted, and he can no longer use his fingerprint to get authenticated. However, he can still use his Smartcard or Personal Password if available. Press **Backspace** to return to Standby mode.	**ID# A01** **Finger Deleted!** **:** **Thu Aug 30 13:50** **ID #:_ IN**

Follow these steps to permanently delete a user from the internal memory:-

Description ***LCD Display***

1. While in the Function Menu, press **4** to select “Del Finger/ID”**.**

```
Del Finger/ID
(1/2)? _
```

2. Enter **2** to select ID. Then you will be asked to enter the user ID to delete.

```
ID to Delete:
A01_
```

3. Press the **Func** key to confirm. The ID # is deleted, and the user can no longer access the system.

   Press **Backspace** to return to Standby mode.

```
ID# A01
Deleted!
```

:

```
Thu Aug 30 13:47
ID #:_        IN
```

Note: Once the user ID is deleted, all the information associated with the user, including the fingerprint data, name, and the access right, will also be permanently deleted. The user must be re-registered to regain access rights. However, access log data will be retained.

Function 5: System Configuration

This is for setting up the system date and time, and for the network configuration, as discussed in the last section, *Getting Started*.

Function 6: Set Password

iGuard has three global passwords:-

- **System Administrator Password** – for system administrator to access the system menu and to configure the system. This password gives full access to the iGuard.

- **User Administrator Password** – for user administrator to manage the user accounts. Specifically, the user administrator can access the Function 1, 2, 3, 4 & 9 in the function menu only. This password does not give access to change the system settings.

- **Door Access Password** – if *Quick Access* mode is enabled, users can use this password to bypass the normal user verification process to release the door strike. This *Quick Access* mode can only be enabled through the web interface, which will be discussed in more detail in the next chapter under the section “*Quick Access*” and “*Password Setup*”.

Follow these steps to assign & edit these passwords:-

Description	***LCD Display***
1. While in Function Menu, press **6** to select “Set Password…”	System Admin: ***_
2. Enter the new System Administrator Password (e.g., AB456). Note that you do not need to press backspace to erase the existing one.	System Admin: *****_
3. Press **Func** to confirm the new password. iGuard will then ask for the User Administrator Password.	User Admin: _
4. Enter the new User Administrator Password and then press **Func** to confirm. Then you will be asked to enter the Door Access Password.	Door Access: _
5. Enter the new Door Access Password and then press **Func** to confirm. The unit will save the new passwords and return to the Standby Mode.	Thu Aug 30 13:48 ID #:_ IN

Note: Both User Administrator Password & Door Access Password are optional. If it is not necessary to assign the password, just press the **Func** key without entering anything to skip the step. However, the System Administrator Password is not optional and must be assigned. The default is 123.

Note: The System Administrator Password of the Slave unit must be the same as the Master unit. Otherwise, the Master unit will reject the slave unit. In this case, an error message will be shown on the LCD display of the slave unit.

Function 7: Shutdown / Reset

Use this function to erase all the user and access log data stored in the internal memory, and to reset all the device settings to the factory default (such as setting the IP address to the default 192.168.0.100, and the terminal name to *iGuard* … etc.).

Follow these steps to reset and shut down the unit:-

Description	***LCD Display***
1. While in Function Menu, press **7** to select “Shutdown / Reset”. You will be asked whether to reset the User Database or not.	Reset User DBase Yes/No (1/2)? _
2. Press **2** to select NO, then you will be asked to reset the Access Log or not.	Reset Access Log Yes/No (1/2)? _
3. Press **2** to select NO, then you will be asked to reset all the settings to factory default or not.	Factory Default Yes/No (1/2)? _

Description **LCD Display**

4. Press **2** to select NO, then the unit will take a few seconds to prepare itself to shut down. Then it will show the message and it is now safe to power off the unit.

```
It is now Safe
To Power Off...
```

Note: When the User Database or the Access Log are reset, all the data will be cleared when the unit is powered up again.

Note: If it is not necessary to reset the data, the device can be shut down safely by simply turning the power off.

Function 8: AutoMatch

Use this function to toggle the AutoMatch option between on and off for a user. AutoMatch enables the device to identify a person without requiring the user to first specify his user ID. This is also called 1-to-Many matching.

Following these steps to set the AutoMatch option for a user:-

Description **LCD Display**

1. While in Function Menu, press **8** to select "AutoMatch". You will be asked to enter the user ID.

```
Enter ID #:
_
```

2. Enter the user ID (e.g., A01)

```
Enter ID #:
A01_
```

3. Press **Func** to confirm. You will see the acknowledge message, and then the unit will return to Standby Mode.

```
ID: A01
AutoMatch Set!
```

:

```
Thu Aug 30 13:50
ID #:_         IN
```

After setting the AutoMatch option, the user no longer needs to enter his ID every time when accessing the device. The user can simply place the finger on the sensor, and iGuard will then automatically capture the image of the finger for authentication.

This feature can be assigned to any user; however, the maximum number of users is 100.

The rest of the users can use ID plus Fingerprint for access.

Please note that users with poor fingerprint quality *should not* use AutoMatch because this option requires a higher quality of fingerprint image.

Follow the same procedure to toggle off this AutoMatch feature for the user.

Function 9: Issue / Import Smartcard

This function is for issuing the optional smartcard to new & existing users, and for importing existing smartcards to a new iGuard.

iGuard comes standard with a built-in contactless smartcard reader, which reads and writes user information to and from the smartcards. The information includes the user names, access right, fingerprint template, and personal password.

Please refer to the procedure on how to issue a Smartcard to new or existing users discussed in the section *Getting Started*.

Note: When issuing a smartcard to an existing user with fingerprint information, only the primary fingerprint is written to the smartcard. This is due to the limited smartcard memory.

There are three possible ways to authenticate a user using Smartcard. These are:

- Smartcard Alone
- Smartcard + Fingerprint
- Smartcard + Personal Password

The first method, *Smartcard Alone*, is already discussed in the chapter *Getting Started* earlier. It is applicable when the unit is in the *Quick Access* mode, or when there is no fingerprint or Personal Password assigned to the smartcard user. In this method, all the user needs to do is to present the smartcard to the unit, and if the user has the access right to the unit, he will get authenticated instantly.

The *Quick Access* Mode is defined in the Web Interface, which will be discussed in the next chapter.

The 2nd method, *Smartcard + Fingerprint*, and the 3rd method, *Smartcard + Personal Password*, are used when the unit is not in the *Quick Access* Mode, and the user has previously enrolled his fingerprint or assigned his Personal Password.

Follow these steps to authenticate users using *Smartcard + Fingerprint* or *Smartcard + Personal Password*:

Description ***LCD Display***

1. While in Standby Mode, present the smart card near the keypad. The unit will read the data stored in the card. If the card is valid, the unit will ask for the Fingerprint Image or the Personal Password to continue…

scrolling message →

```
A02
Waiting Finger/P
```

:

```
A02
Password... Wait
```

2. To authenticate using fingerprint, place either your primary finger or your secondary finger on the sensor. To authenticate using Personal Password, simply enter the Personal Password and press **Func** to confirm.

```

Scanning...
```

- or -

```
Your Password:
****_
```

Description	***LCD Display***
3. If the Fingerprint or the Personal Password matches the record, the user will be authenticated, and the unit will return to the Standby Mode.	**A02** **Authorized!** **:** **Thu Aug 30 13:50** **ID #:_ IN**

This *Function 9* can also be used to import (register) an existing smartcard user to another iGuard unit.

This is useful if there are remote locations that are not tied into the master unit via a WAN of some kind, users of these remote locations can register to the master unit by importing their existing smartcards, rather than registering the fingerprint and other information to the unit once again, since all the information is already available in the smartcards.

Follow these steps to register an existing Smartcard user with the smartcard:-

Description	***LCD Display***
1. While in Function Menu, press **9** to select “Issue / Import Card”.	**Issue/Import** **Card (1/2)? _**
2. Press **2** to select “Import Card”, then you will be prompted to present the user’s existing Smartcard.	**Waiting for** **SmartCard...**
3. If the Smartcard is valid, the information stored in the Smartcard, including the user name, fingerprint template, access right…etc., will be read and saved in the unit. The unit will then wait for the next Smartcard.	**ID: A02** **Added OK!** **:** **Waiting for** **SmartCard...**
4. Press **Backspace** to return to the Standby Mode.	**Thu Aug 30 13:55** **ID #:_ IN**

Please note that the administrator may still need to grant the user’s access rights by assigning the departments the user belongs to.

Note: “Department” is used for assigning access rights to different users at different time & terminals. Please refer to the section “Department” in the next chapter, *Using The Web Browser*, on page 46 for more information.

Function 0: Advanced Feature

This function contains a number of handy tools for setup and network diagnosis.

1. Ping Test

This test is analogous to the ping test in PC. It comes in handy when it is necessary to test the connection between the iGuard and a PC, for example.

Description	***LCD Display***

1. While in Function Menu, press **0** to select *"Advanced Feature"*. Then you will be asked if you want to perform a Ping Test.	`Ping Test`
	`Yes/No (1/2)? _`

2. Press **1** to select YES, then you will be asked to enter the IP address of the target device. Enter the IP address of the target device.	`IP Address:`
	`192.168.000.123`

3. Press **Func** to confirm. The unit will try to ping the target device, and display the result as shown.	`192.168.000.123`
	`Ping:#1 5ms`
	:
	`192.168.000.123`
	`Ping:#3 7ms`

4. Press **Backspace** to return to the Standby Mode.	`Thu Aug 30 13:57`
	`ID #:_        IN`

2. Reset FP Sensor (Reset Fingerprint Sensor)

In an unlikely event that the automatch feature does not work properly, it would be helpful to reset the fingerprint sensor and re-index the automatch records as follows:

Description	***LCD Display***

1. While in Function Menu, press **0** to select "Advanced Feature". Then press **2** to skip to "Reset FP Sensor".	`Reset FP Sensor`
	`Yes/No (1/2)? _`

2. Press **1** to select YES, then the reset process will start immediately.	`Setting Up`
	`AutoMatch 01/65`

3. It will return to the Standby Mode when the process is finished.	`Thu Aug 30 13:57`
	`ID #:_        IN`

Function A: Test Mode Toggle

By default, iGuard records all the user access in the Access Log. The device can be set to the ***Test Mode***, and it will temporarily stop recording the transactions.

This feature comes in handy when, for example, someone wants to "practice" with or test the device by clocking in and out with the fingerprint, but does not want to include these records in the access log.

Follow these steps to toggle the test mode:-

Description	***LCD Display***

1. While in Function Menu, press **A** to toggle the device to Test Mode. The unit will return to Standby Mode, and the "*Test Mode*" status will appear on the 1st line as shown.	`== Test Mode! ==`
	`ID #:_        IN`

2. Repeat the above step and the unit will return to the normal Standby mode.	`Thu Aug 30 14:15`
	`ID #:_        IN`

Note: The *"Test Mode"* must be toggled back to *"Normal Mode"* before the unit will begin to record transactions in the access log again.

Function B: Open Door

This is for the System Administrator to quickly open the door without going through all the verification procedure.

This feature has been added as a backup mean to open the door. In the unlikely event when the iGuard fails to read any smartcard or fingerprint image due to hardware failure, the System Administrator can still have a way to open the door.

Description	***LCD Display***

1. While in Function Menu, press **B** to open the door. The door will then open and unit will return to the Standby Mode.	`Open Door!`
	`:`
	`Thu Aug 30 14:17`
	`ID #:_        IN`

The Backspace Key

The backspace key on the keypad mainly serves three functions: to erase the last entered key, to abort in the middle of an operation, and to toggle the access status between IN and OUT during Standby Mode. This section will discuss how to use the Backspace key to toggle the access status.

The default access status is IN, as shown in the 2nd line of the LCD display when the unit is in Standby Mode. Follow the steps below to change the access status from the default IN to OUT:-

Description ***LCD Display***

1. In Standby Mode, the default access status is shown in the 2nd line of the display (which is IN in this case).

```
Thu Aug 30 16:36
ID #:_        IN
```

2. Press the **Backspace** key and the access status will be changed to OUT. Then follow the usual procedure to continue (e.g. enter the user ID and present the smartcard).

```
Thu Aug 30 16:36
ID #:_       OUT
```

3. If no key is pressed for approximately 5 seconds, the unit will show the *Time Out* message, and will return to the default access status.

```

Time Out!
```

:

```
Thu Aug 30 16:36
ID #:_        IN
```

Note: The default access status can be set to either IN or OUT in the *"In / Out Trigger"* page via the web browser. More detail can be found on page 57.

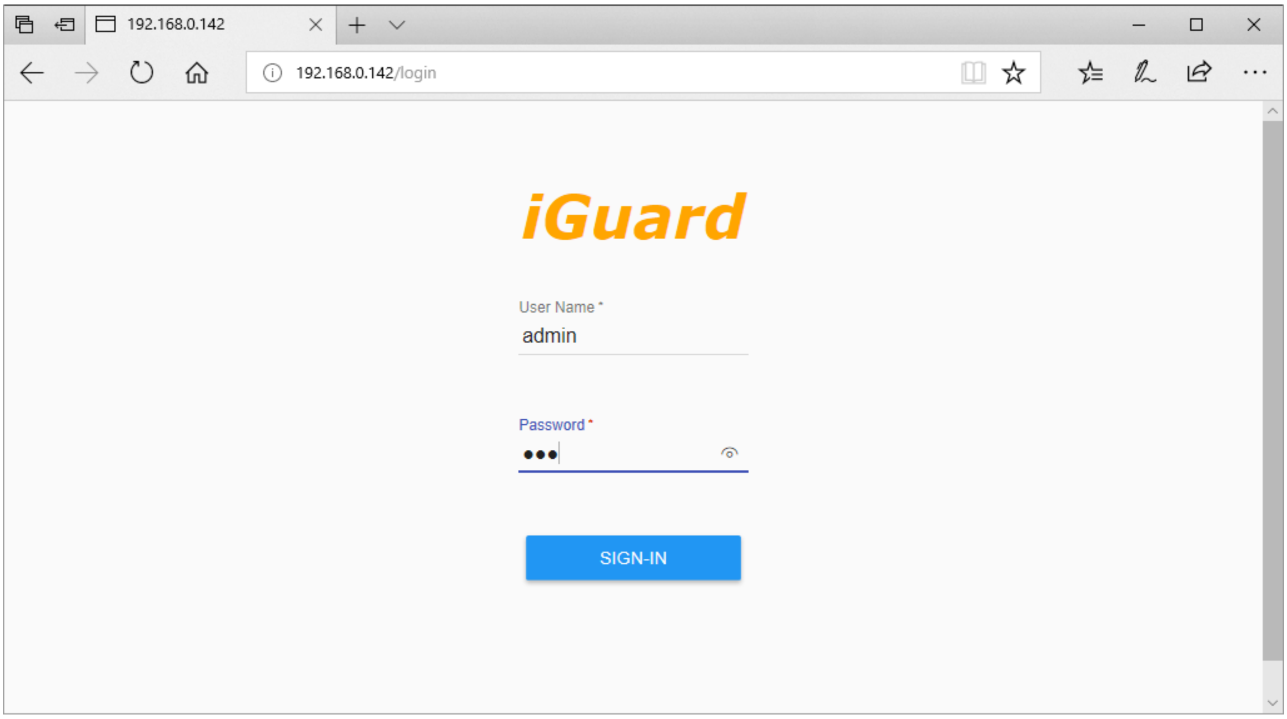
USING THE WEB BROWSER

iGuard has a built-in web server which operates exactly like a hosted web site. The web interface gives the system administrator a simple, easy to use set of tools to configure and maintain the unit and the users. Retrieve the access log records and other data with any standard web browser, such as Chrome, Microsoft Edge and Firefox.

With this feature, the unit may be accessed by any PC connected to the corporate network, without the need for any dedicated PC or any special software package. If the iGuard is connected to the Internet, it can even be accessed from anywhere in the world via the Internet.

iGuard is platform independent. It can be a Windows-based machine running Microsoft Windows Vista, a Linux machine or an Apple iMac machine, as long as it runs the standard web browser.

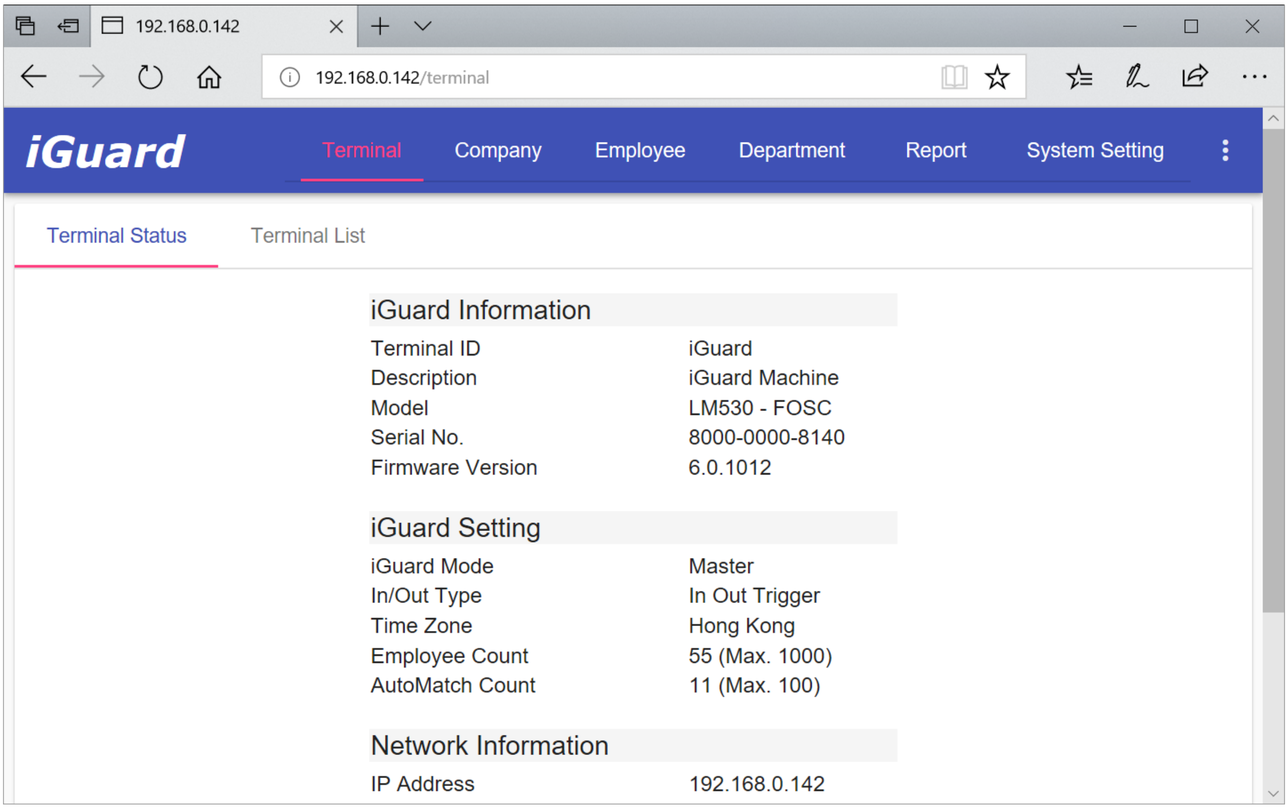
Once connected to the corporate computer network, the unit may be accessed by specifying the IP address in the Web Browser (e.g., http://192.168.0.142). This is the IP address assigned to the iGuard during the setup procedure previously discussed. The following Login page will appear in the browser: -



Enter the default user name and password to log in.

Note: The default user name and password are `admin` and `123`. This password is the same as the System Administrator password discussed **"Function 6"** in the last section. Use the new password if it has been changed.

After logging in, the following screen will appear, with the system information including Terminal ID, Model, Serial No., Firmware Version… etc.



iGuard Information

Terminal ID	iGuard
Description	iGuard Machine
Model	LM530 - FOSC
Serial No.	8000-0000-8140
Firmware Version	6.0.1012

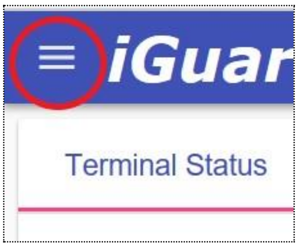
iGuard Setting

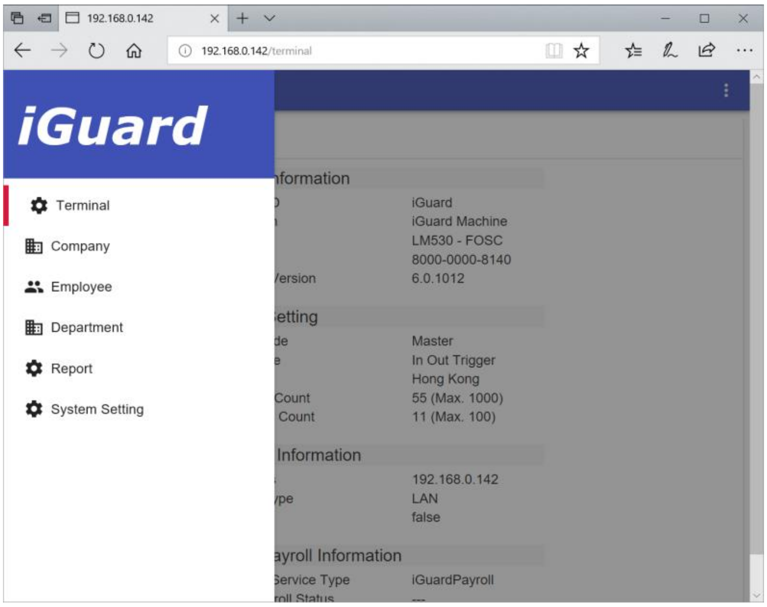
iGuard Mode	Master
In/Out Type	In Out Trigger
Time Zone	Hong Kong
Employee Count	55 (Max. 1000)
AutoMatch Count	11 (Max. 100)

Network Information

IP Address	192.168.0.142

Different items can be selected in the top menu or in the “Hamburger” pull-down menu (as shown below), depending the browser’s screen width:





There are six items in the menu. This chapter will discuss each of these items in detail.

Terminal

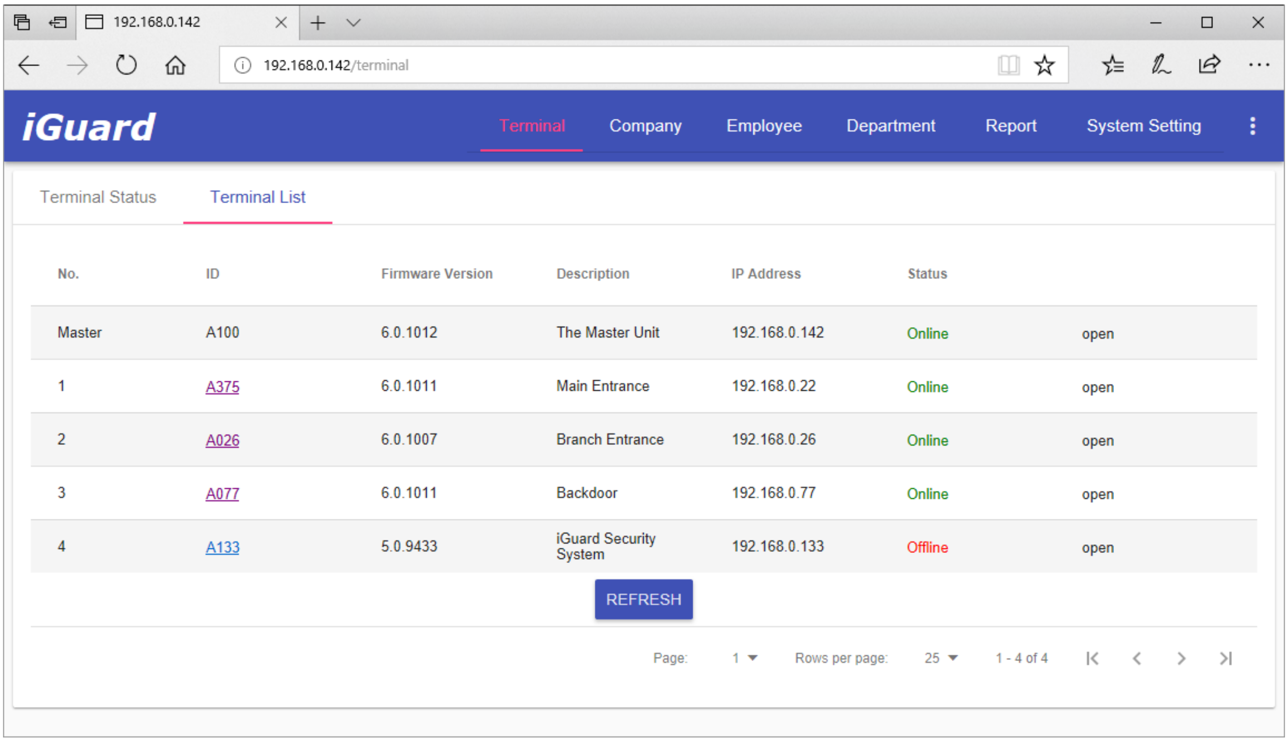
The status of the iGuard unit and a list of the other units exist in the same Master / Slave network are shown in this menu item.

Terminal Status

This page shows a quick reference for various information, including the Terminal ID, Description, Model, Serial No., Firmware Version, and more…

Terminal List

This page shows the iGuard List in a **Master / Slave** network. The following is a screen shot of a particular **Master** unit:



No.	ID	Firmware Version	Description	IP Address	Status	
Master	A100	6.0.1012	The Master Unit	192.168.0.142	Online	open
1	A375	6.0.1011	Main Entrance	192.168.0.22	Online	open
2	A026	6.0.1007	Branch Entrance	192.168.0.26	Online	open
3	A077	6.0.1011	Backdoor	192.168.0.77	Online	open
4	A133	5.0.9433	iGuard Security System	192.168.0.133	Offline	open

Master Mode

In the above example, the device “A100” is the master unit, and it has four slave units with terminal ID “A375”, “A026”, “A077” & “A133”.

The corresponding Firmware Version, IP address & the Port number are also shown.

The Network Status column indicates the network connection status. In the above example, the slave unit “A133” is offline.

As a convenient feature, one can remotely unlock the doors of the slave unit by clicking the corresponding “**Open**” link.

Click on the “**Refresh**” button at the end of the list to refresh the screen. This is useful for updating the online / offline status of the slave units.

Slave Mode

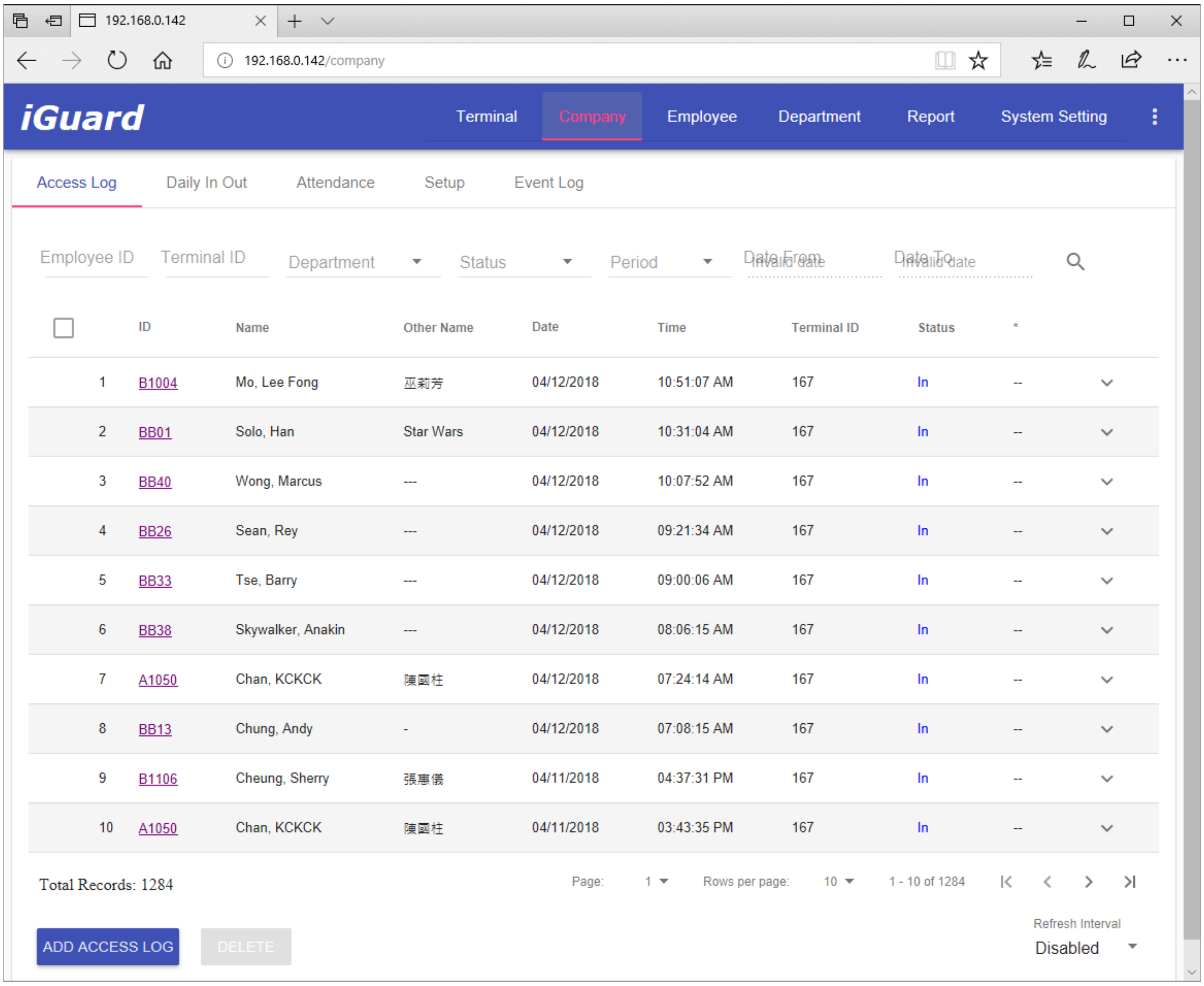
For iGuard in the **Slave** Mode: This page shows the relevant information of the Master unit connected, as well as the slave unit itself.

Company

The Company tab consists of *Company Reports* including *Access Log*, *Daily In Out*, *Attendance*, *Setup* and *Event Log*.

Access Log

Access Log is the first item in the Company tab, as shown in the following screenshot:



□	ID	Name	Other Name	Date	Time	Terminal ID	Status	*
1	B1004	Mo, Lee Fong	巫莉芳	04/12/2018	10:51:07 AM	167	In	--
2	BB01	Solo, Han	Star Wars	04/12/2018	10:31:04 AM	167	In	--
3	BB40	Wong, Marcus	---	04/12/2018	10:07:52 AM	167	In	--
4	BB26	Sean, Rey	---	04/12/2018	09:21:34 AM	167	In	--
5	BB33	Tse, Barry	---	04/12/2018	09:00:06 AM	167	In	--
6	BB38	Skywalker, Anakin	---	04/12/2018	08:06:15 AM	167	In	--
7	A1050	Chan, KCKCK	陳國柱	04/12/2018	07:24:14 AM	167	In	--
8	BB13	Chung, Andy	-	04/12/2018	07:08:15 AM	167	In	--
9	B1106	Cheung, Sherry	張惠儀	04/11/2018	04:37:31 PM	167	In	--
10	A1050	Chan, KCKCK	陳國柱	04/11/2018	03:43:35 PM	167	In	--

Total Records: 1284

Page: 1 Rows per page: 10 1 - 10 of 1284

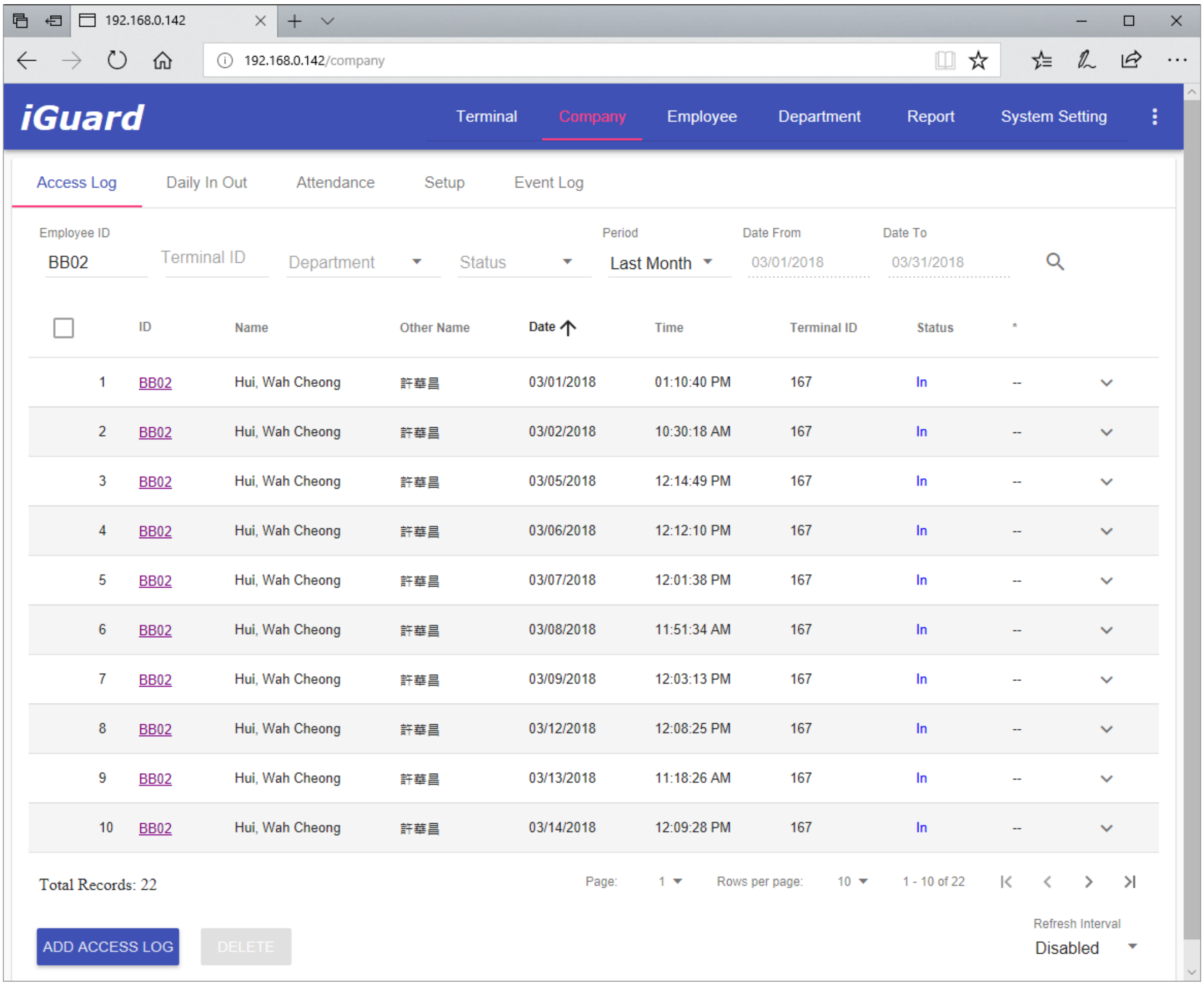
Refresh Interval Disabled

This page shows the Access Log of the employees' clock-in & clock-out records. iGuard keeps the most recent 20,000 access log records in the internal database based on the First-IN-First-OUT rule. When the number of access log records exceeds 20,000, iGuard will delete the oldest record automatically to make room for the new one.

To show the records of a particular employee only (e.g., BB02), enter her ID # in the *Employee ID* text box and press the **Search** button (i.e., the magnifying-glass icon), and only the records of this person will be shown. Similarly, specifying the *Department* and only the particular department members will be shown.

The *Period* may be specified such as displaying only *today's* records, *last week* records, *last month* records… etc., or specify the Time Period by choosing the *Range* selection and entering directly to the *Date From / Date To* fields.

The following example shows only the *Last Month* records of the employee ID # BB02 (ordered by Date):



Employee ID: BB02
Terminal ID
Department
Status
Period: Last Month
Date From: 03/01/2018
Date To: 03/31/2018

□	ID	Name	Other Name	Date ↑	Time	Terminal ID	Status	*
1	BB02	Hui, Wah Cheong	許華昌	03/01/2018	01:10:40 PM	167	In	--
2	BB02	Hui, Wah Cheong	許華昌	03/02/2018	10:30:18 AM	167	In	--
3	BB02	Hui, Wah Cheong	許華昌	03/05/2018	12:14:49 PM	167	In	--
4	BB02	Hui, Wah Cheong	許華昌	03/06/2018	12:12:10 PM	167	In	--
5	BB02	Hui, Wah Cheong	許華昌	03/07/2018	12:01:38 PM	167	In	--
6	BB02	Hui, Wah Cheong	許華昌	03/08/2018	11:51:34 AM	167	In	--
7	BB02	Hui, Wah Cheong	許華昌	03/09/2018	12:03:13 PM	167	In	--
8	BB02	Hui, Wah Cheong	許華昌	03/12/2018	12:08:25 PM	167	In	--
9	BB02	Hui, Wah Cheong	許華昌	03/13/2018	11:18:26 AM	167	In	--
10	BB02	Hui, Wah Cheong	許華昌	03/14/2018	12:09:28 PM	167	In	--

Total Records: 22
Page: 1 Rows per page: 10 1 - 10 of 22

ADD ACCESS LOG DELETE

Refresh Interval: Disabled

You can navigate to different page, or jump to a particular page, of the Access Log through the navigation at the end of the page.

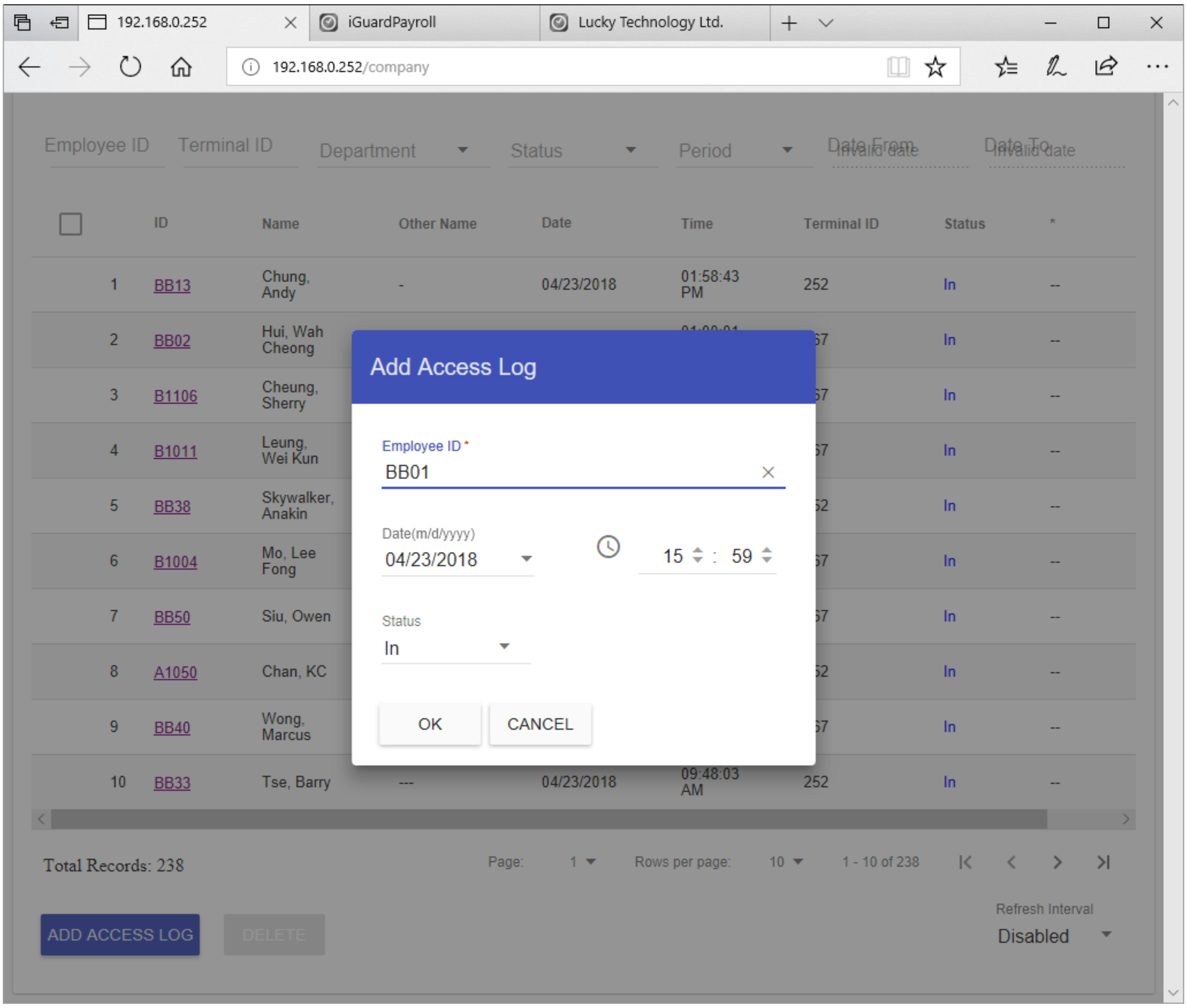
This page can automatically refresh itself periodically to fetch and display the latest log by setting the **Refresh Interval** at the bottom of the page. Available refresh interval options are 5, 10 & 20 seconds.

Add Access Log

It is sometimes necessary to add a record manually for an employee. For example, the employee might have forgotten to clock-out before going home at the end of the day, and therefore it is necessary to make up for the mistake by manually adding this entry back, which is particularly useful for payroll purposes.

By default, only access records which have been manually added can be changed or deleted.

Press the **ADD ACCESS LOG** button to add an access log manually, as shown is the following screenshot:



Employee ID | Terminal ID | Department | Status | Period | Date From Invalid date | Date To Invalid date

□	ID	Name	Other Name	Date	Time	Terminal ID	Status	*
1	BB13	Chung, Andy	-	04/23/2018	01:58:43 PM	252	In	--
2	BB02	Hui, Wah Cheong				67	In	--
3	B1106	Cheung, Sherry				67	In	--
4	B1011	Leung, Wei Kun				67	In	--
5	BB38	Skywalker, Anakin				52	In	--
6	B1004	Mo, Lee Fong				67	In	--
7	BB50	Siu, Owen				67	In	--
8	A1050	Chan, KC				52	In	--
9	BB40	Wong, Marcus				67	In	--
10	BB33	Tse, Barry	---	04/23/2018	09:48:03 AM	252	In	--

Total Records: 238 Page: 1 Rows per page: 10 1 - 10 of 238

ADD ACCESS LOG DELETE

Refresh Interval: Disabled

Add Access Log

Employee ID *: BB01

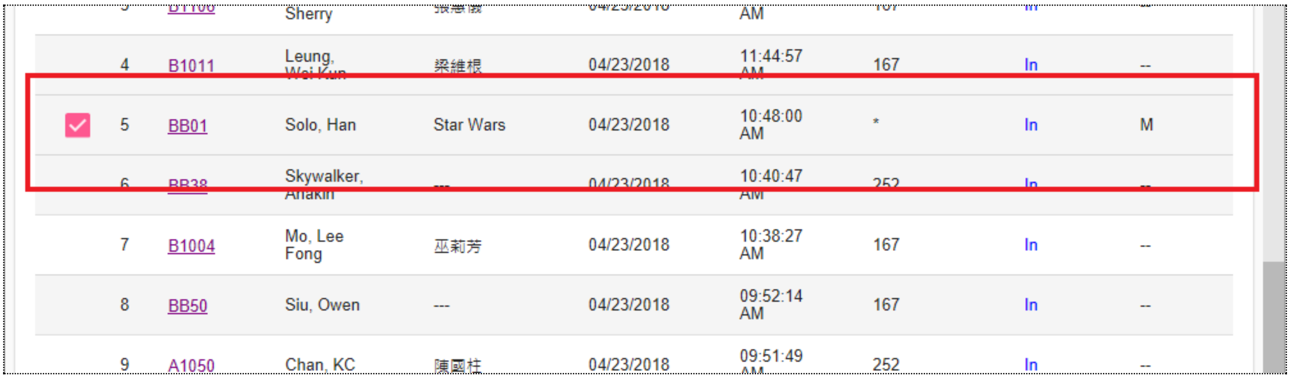
Date(m/d/yyyy): 04/23/2018 15 : 59

Status: In

OK CANCEL

Delete Access Log

The **Delete** button is for deleting the selected Access Logs.

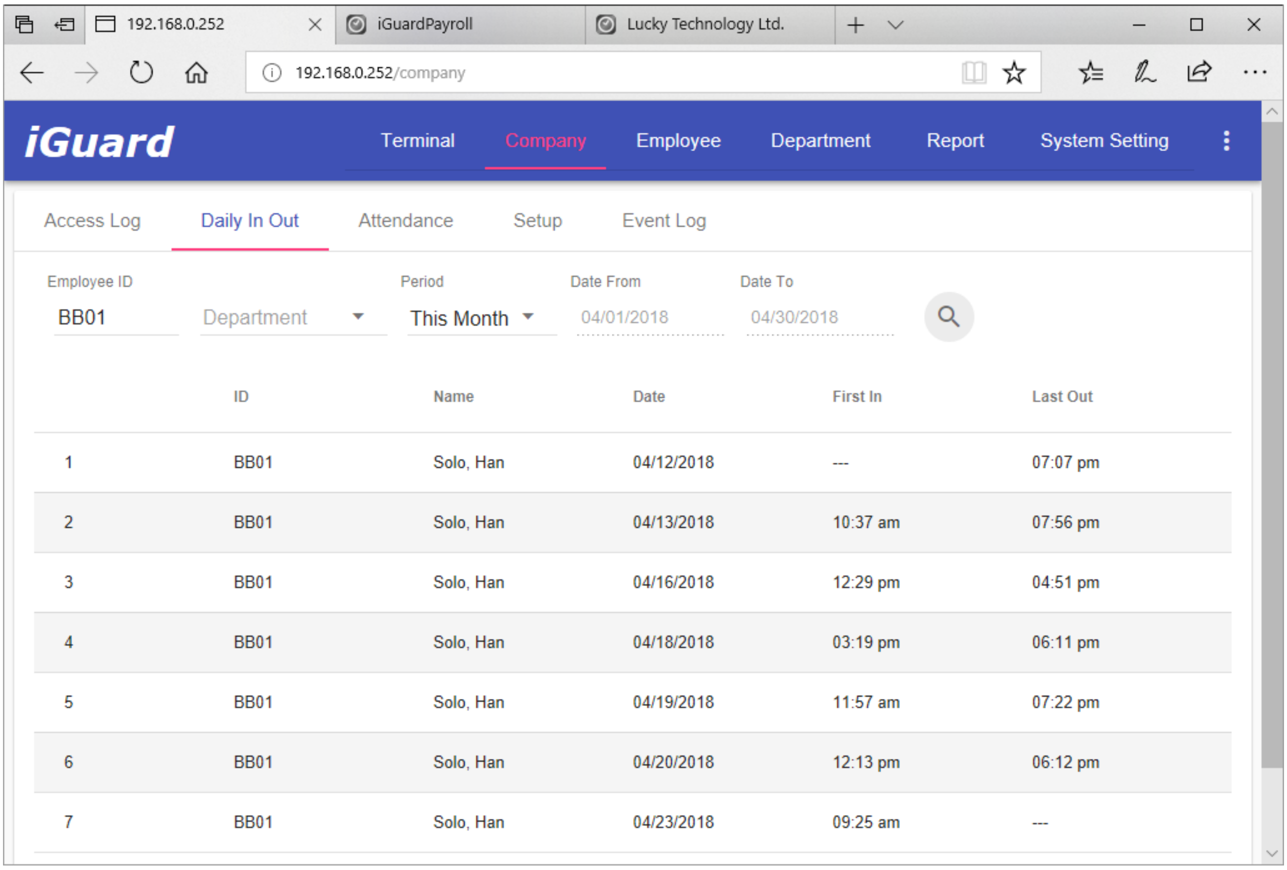


	4	B1011	Leung, Wei Kun	梁維根	04/23/2018	11:44:57 AM	167	In	--
☑	5	BB01	Solo, Han	Star Wars	04/23/2018	10:48:00 AM	*	In	M
	6	BB38	Skywalker, Anakin	---	04/23/2018	10:40:47 AM	252	In	--
	7	B1004	Mo, Lee Fong	巫莉芳	04/23/2018	10:38:27 AM	167	In	--
	8	BB50	Siu, Owen	---	04/23/2018	09:52:14 AM	167	In	--
	9	A1050	Chan, KC	陳國柱	04/23/2018	09:51:49 AM	252	In	--

Note: Only manually added logs can be selected and deleted. All other access log records created normally are irrevocable.

Daily In Out

The Daily In / Out Report is similar to the Access Log Report above, except that it only shows the first IN time and the last OUT time for the day as shown below:

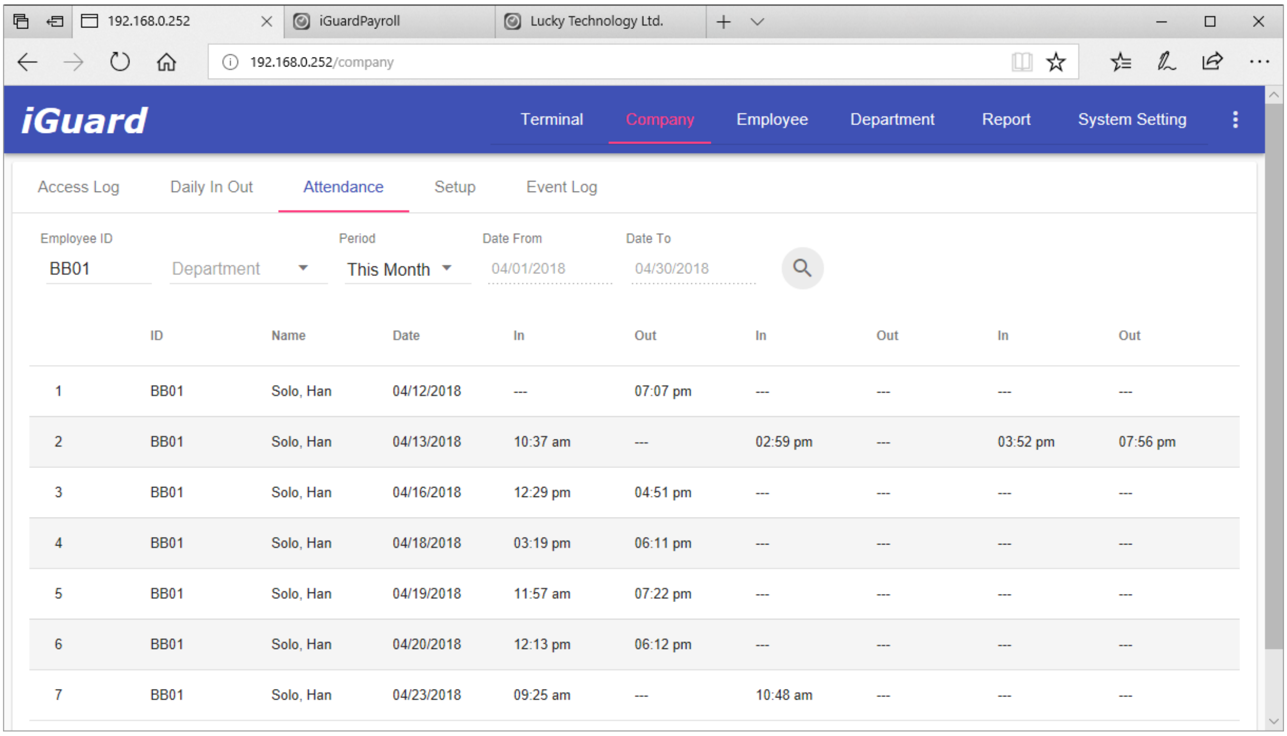


Employee ID: BB01 | Department | Period: This Month | Date From: 04/01/2018 | Date To: 04/30/2018

	ID	Name	Date	First In	Last Out
1	BB01	Solo, Han	04/12/2018	---	07:07 pm
2	BB01	Solo, Han	04/13/2018	10:37 am	07:56 pm
3	BB01	Solo, Han	04/16/2018	12:29 pm	04:51 pm
4	BB01	Solo, Han	04/18/2018	03:19 pm	06:11 pm
5	BB01	Solo, Han	04/19/2018	11:57 am	07:22 pm
6	BB01	Solo, Han	04/20/2018	12:13 pm	06:12 pm
7	BB01	Solo, Han	04/23/2018	09:25 am	---

Attendance

The attendance report provides a consolidated access records of each employee:



Employee ID: BB01 | Department | Period: This Month | Date From: 04/01/2018 | Date To: 04/30/2018

	ID	Name	Date	In	Out	In	Out	In	Out
1	BB01	Solo, Han	04/12/2018	---	07:07 pm	---	---	---	---
2	BB01	Solo, Han	04/13/2018	10:37 am	---	02:59 pm	---	03:52 pm	07:56 pm
3	BB01	Solo, Han	04/16/2018	12:29 pm	04:51 pm	---	---	---	---
4	BB01	Solo, Han	04/18/2018	03:19 pm	06:11 pm	---	---	---	---
5	BB01	Solo, Han	04/19/2018	11:57 am	07:22 pm	---	---	---	---
6	BB01	Solo, Han	04/20/2018	12:13 pm	06:12 pm	---	---	---	---
7	BB01	Solo, Han	04/23/2018	09:25 am	---	10:48 am	---	---	---

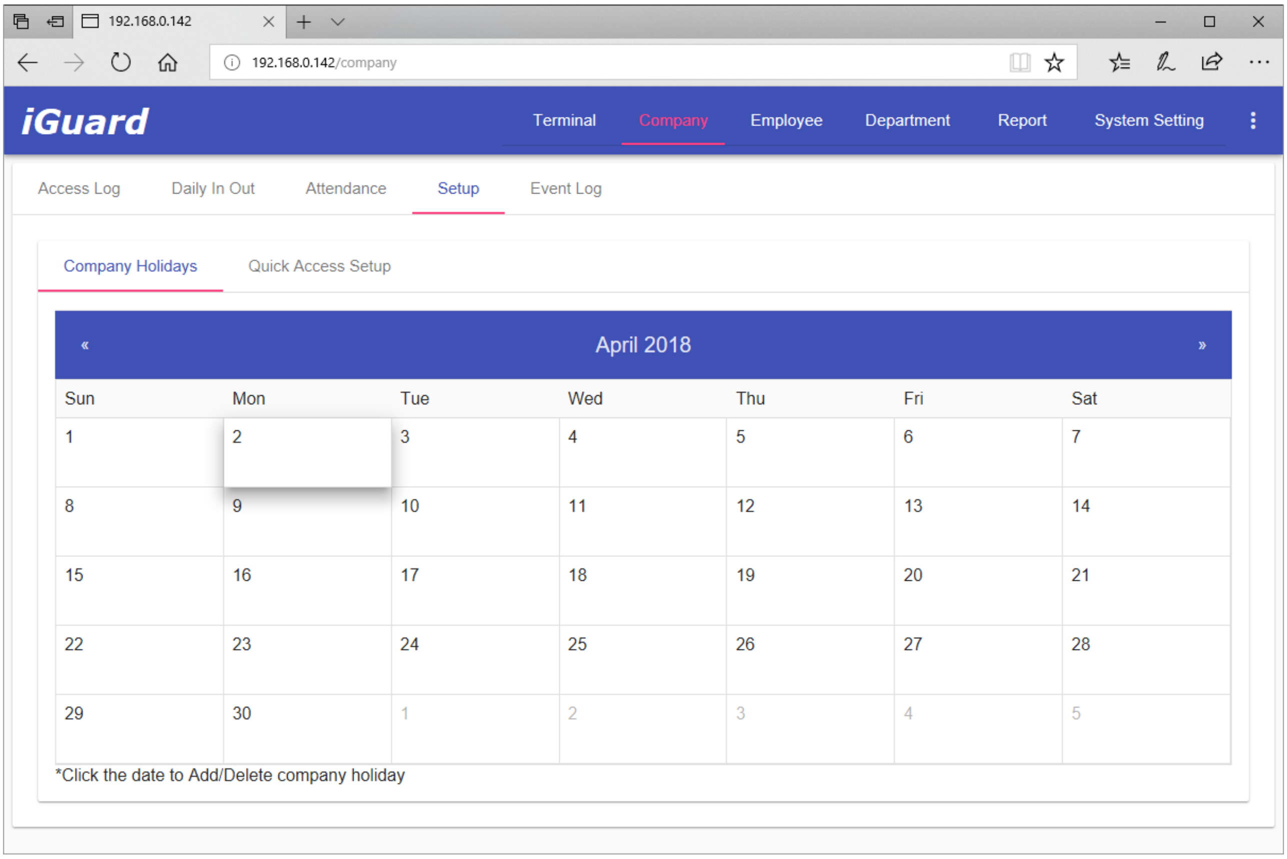
The Attendance Report shows the first three in-out-time pairs of each day, and is particularly useful for payroll purpose. Similar to the other reports above, the employee's ID and/or the Time Period of the Attendance Report can be specified.

Setup

This page consists of two subpages: Company Holidays and Quick Access.

Company Holidays

Use this page to assign Company Holidays. "Company Holidays" is a list used for the time restriction purpose (along with the day-of-week settings) for access right control. The following is a typical example of the setting:



April 2018

Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5

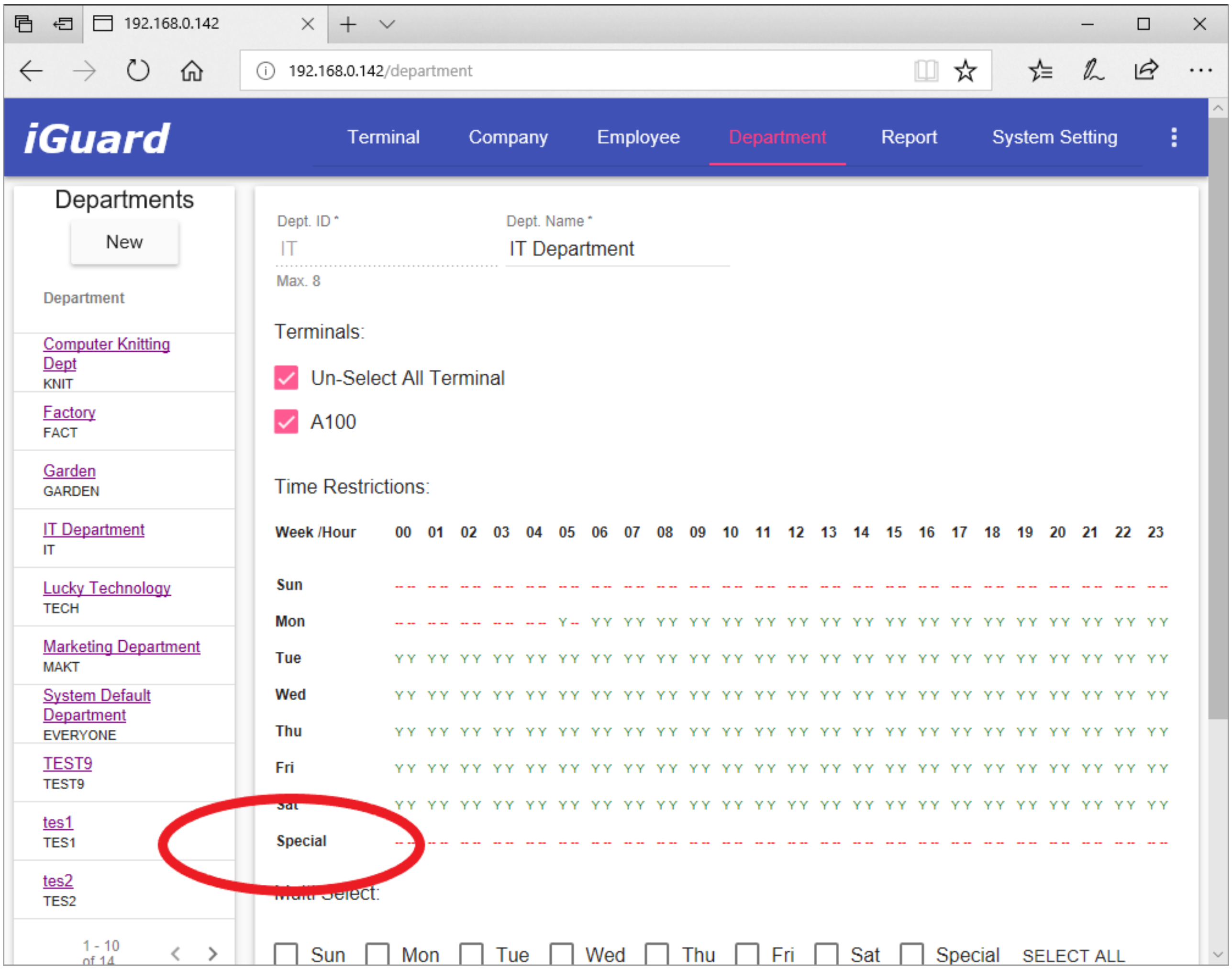
*Click the date to Add/Delete company holiday

Click on a date to set it as a holiday. Click on it again to remove it from the holiday.

Do not confuse the Company Holidays discuss here with the one found in the *iGuardPayroll* cloud service.

As an example, if "April 2, 2018" is set as a company holiday, the authorized time period will follow the settings for the date "*Special*" in the **Departments**[6] page as follows:

[6] Departments will be covered on page 46.



Department

Computer Knitting Dept
KNIT

Factory
FACT

Garden
GARDEN

IT Department
IT

Lucky Technology
TECH

Marketing Department
MAKT

System Default Department
EVERYONE

TEST9
TEST9

tes1
TES1

tes2
TES2

Dept. ID *: IT
Max. 8

Dept. Name *: IT Department

Terminals:

☑ Un-Select All Terminal

☑ A100

Time Restrictions:

Week /Hour	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sun	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Mon	--	--	--	--	--	Y-	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY
Tue	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY
Wed	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY
Thu	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY
Fri	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY
Sat	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY
Special	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Multi Select:

□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Special SELECT ALL

Quick Access Setup

Quick Access is an access control feature of iGuard which, when activated, allows users to come and go without authenticating individually. The system administrator can authorize this *Quick Access* period by specifying the time, dates and the terminals.

There are three ways to utilize this feature:-

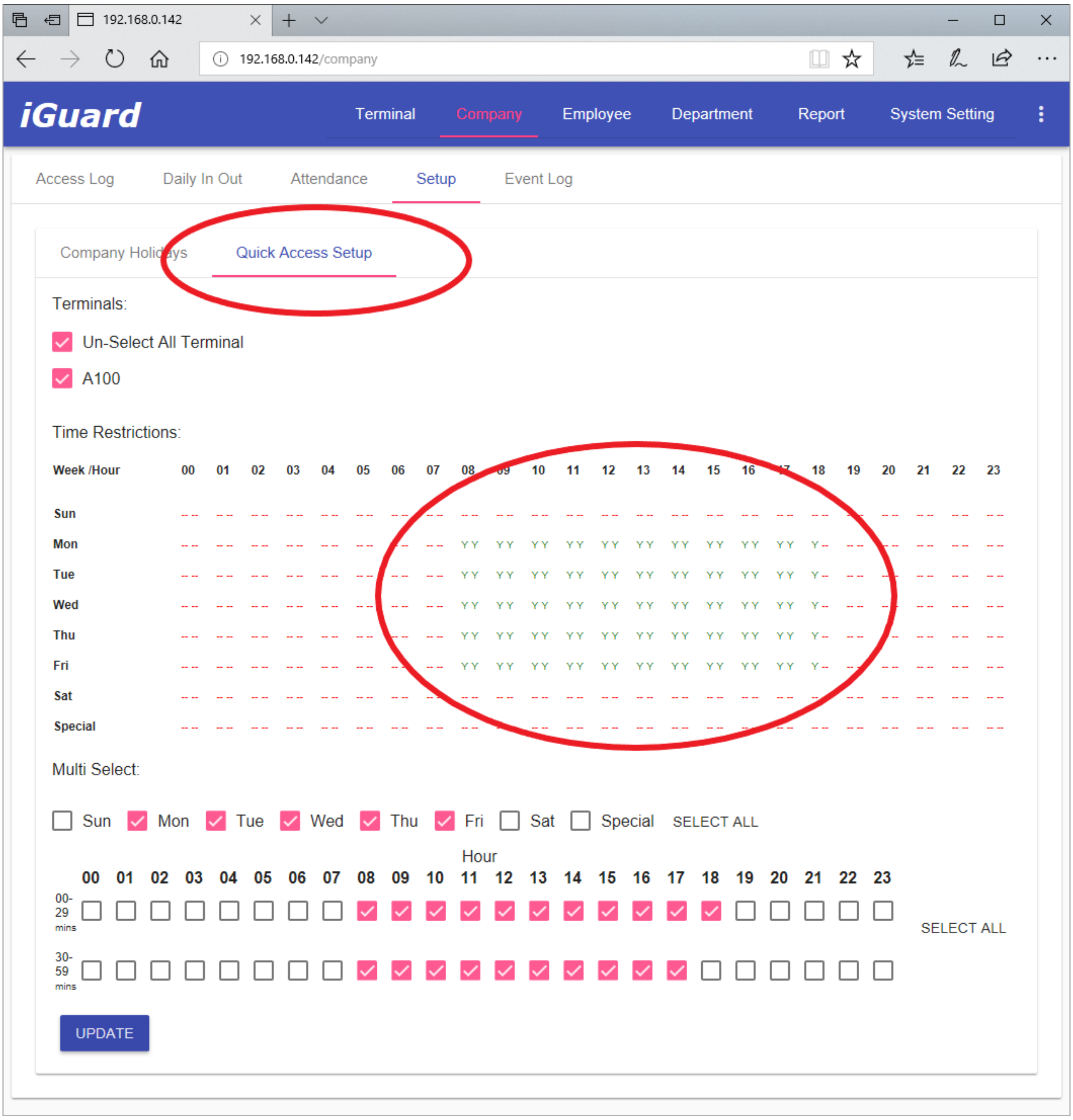
- *Quick Access Password*[7] – This password can be given to Emergency Medical Services, building maintenance, or your mail carrier. This can be useful if it is necessary to keep the facility locked but without the need to record the individuals who are coming and going during business hours.

- *Smartcards* – For users with smartcards, this *Quick Access* will let them enter and exit with the smartcard, and will not ask for fingerprint or personal password.

In a typical setting, one can enable this *Quick Access* period during the normal office hour when the traffic is high and the security requirement is low, and disable the *Quick Access* otherwise. In this setting, users only need to present their smartcards to get authenticated to speed up the authentication process. But they need to use both Smartcards and Fingerprint or Personal Password during the other time that requires higher security level.

[7] Quick Access Password can be setup at *System Setting* → *Account* (p. 58)

Use this page to define the authorized *Quick Access* period and the corresponding iGuard units. The default setting is NONE, i.e., there are no authorized terminals or access times for *Quick Access*.



Terminals:

☑ Un-Select All Terminal

☑ A100

Time Restrictions:

Week /Hour	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sun	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Mon	--	--	--	--	--	--	--	--	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	Y-	--	--	--	--	--
Tue	--	--	--	--	--	--	--	--	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	Y-	--	--	--	--	--
Wed	--	--	--	--	--	--	--	--	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	Y-	--	--	--	--	--
Thu	--	--	--	--	--	--	--	--	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	Y-	--	--	--	--	--
Fri	--	--	--	--	--	--	--	--	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	Y-	--	--	--	--	--
Sat	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Special	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Multi Select:

□ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat □ Special SELECT ALL

Hour

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
00-29 mins	□	□	□	□	□	□	□	□	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	□	□	□	□	□
30-59 mins	□	□	□	□	□	□	□	□	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	□	□	□	□	□	□

SELECT ALL

UPDATE

The procedure for setting the valid period for Quick Access is similar to the procedure for setting up the departments, which is under the Department tab in the top menu.

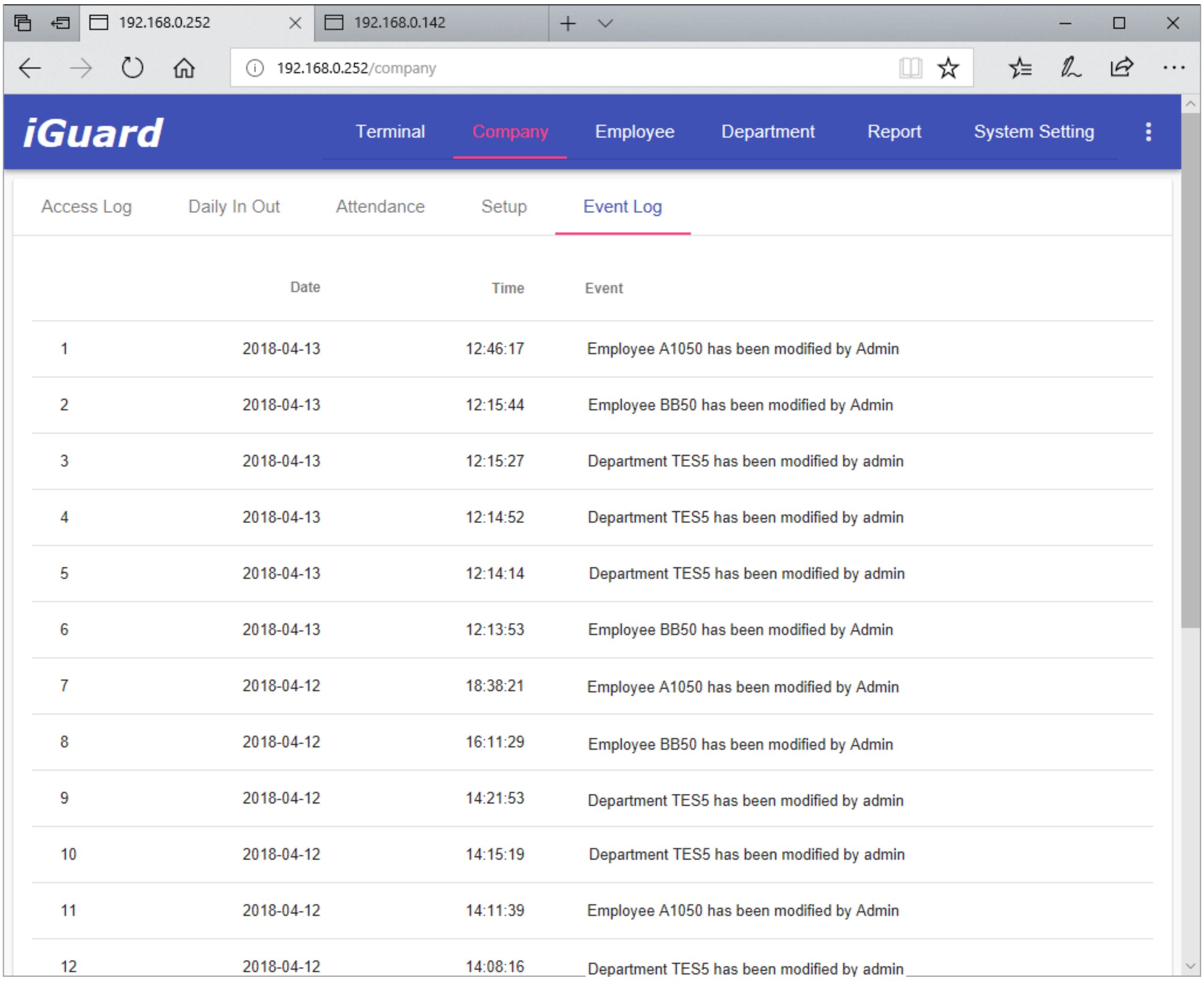
In the above example, Quick Access is available from 8:00AM until 6:30PM Monday through Friday, and not on Sunday, Saturday, and other specified company holidays.

Event Log

This page shows the history of iGuard's alerts and notifications, including the following items:

- Adding and Modifying Employees
- Changing System Settings
- System Start
- Other record updates
- System Errors

The following is a sample of the event log:



	Date	Time	Event
1	2018-04-13	12:46:17	Employee A1050 has been modified by Admin
2	2018-04-13	12:15:44	Employee BB50 has been modified by Admin
3	2018-04-13	12:15:27	Department TES5 has been modified by admin
4	2018-04-13	12:14:52	Department TES5 has been modified by admin
5	2018-04-13	12:14:14	Department TES5 has been modified by admin
6	2018-04-13	12:13:53	Employee BB50 has been modified by Admin
7	2018-04-12	18:38:21	Employee A1050 has been modified by Admin
8	2018-04-12	16:11:29	Employee BB50 has been modified by Admin
9	2018-04-12	14:21:53	Department TES5 has been modified by admin
10	2018-04-12	14:15:19	Department TES5 has been modified by admin
11	2018-04-12	14:11:39	Employee A1050 has been modified by Admin
12	2018-04-12	14:08:16	Department TES5 has been modified by admin

In addition, should technical support be required, it would be helpful to provide this event log for the technical support.

Employee

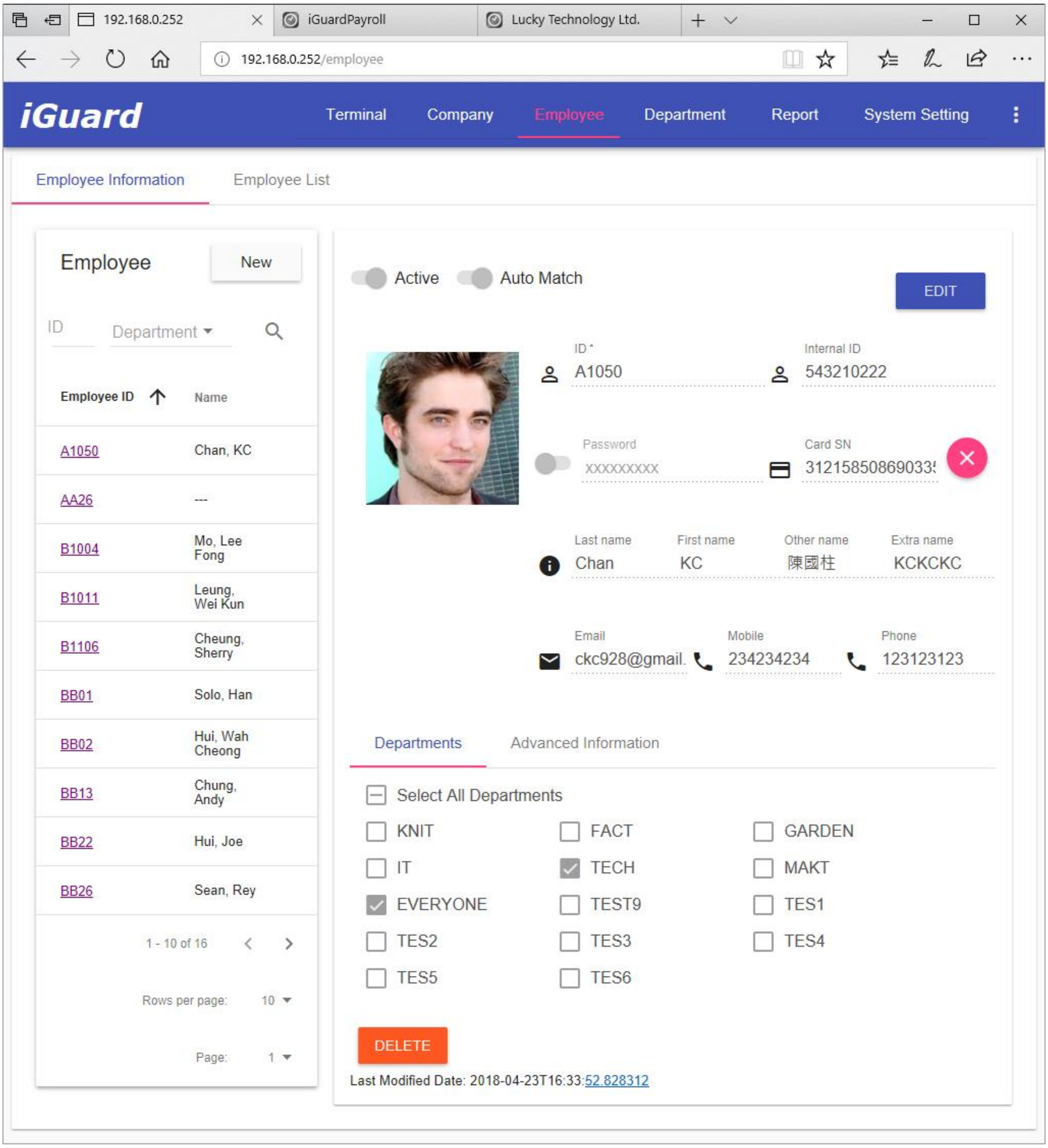
The Employee menu is for maintaining the employee information of the company. It consists of *Employee List* page for listing all registered employees, and *Employee Information* page for maintaining each individual employee.

The maximum number of employee is 1,000, and is shown in the *Terminal Status* page discussed before.

Please contact the dealer or the manufacturer for higher capacity. Available options are 5,000, 10,000 and 20,000 employees.

Employee Information

Use this page to retrieve and/or edit the employee information. To edit the information, press the Edit button at the upper right corner.



Employee ID	Name
A1050	Chan, KC
AA26	---
B1004	Mo, Lee Fong
B1011	Leung, Wei Kun
B1106	Cheung, Sherry
BB01	Solo, Han
BB02	Hui, Wah Cheong
BB13	Chung, Andy
BB22	Hui, Joe
BB26	Sean, Rey

1 - 10 of 16

Rows per page: 10

Page: 1

Active
Auto Match

ID *: A1050
Internal ID: 543210222
Password: XXXXXXXXX
Card SN: 31215850869033!
Last name: Chan
First name: KC
Other name: 陳國柱
Extra name: KCKCKC
Email: ckc928@gmail.
Mobile: 234234234
Phone: 123123123

□ Select All Departments

□ KNIT
□ IT
☑ EVERYONE
□ TES2
□ TES5
□ FACT
☑ TECH
□ TEST9
□ TES3
□ TES6
□ GARDEN
□ MAKT
□ TES1
□ TES4

Last Modified Date: 2018-04-23T16:33:52.828312

Active – The default user status is *Active*. Turn it off if it is necessary to temporarily suspend the user's access rights.

AutoMatch – Turn it on to include this user in the AutoMatch group for the 1-to-many fingerprint matching.

ID – This is the Employee ID, which is a unique value, up to 10 characters, and is limited to the characters 0-9, A, and B. The limitation is due to the keypad: these are the only characters on the keypad of the iGuard unit.

Internal ID – Optional identity number for the employee, such as the existing company ID.

Password – Enter the Personal Password of the employee.

Card SN – This is the serial number of the employee's SmartCard. Each SmartCard has a unique serial number, and it is used to identify the employee. This field is read-only and cannot be modified. However, it can be removed in order to free this card for another employee. To remove the SmartCard, simply click on the "cross" button next to the field.

Last Name & First Name – Enter the first and last name of the employee.

Other Name & Extra Name – These two fields are for extra information, such as the Chinese Name, etc.

Email, Mobile & Phone – these are the optional fields for the employees.

Profile Picture – Profile Picture is optionally included in each employee's record. A new profile picture of the employee can be uploaded in the Edit page.

In addition, there are two tabs labeled **Departments** and **Advanced Information**:

Departments

This is to assign the user to different departments by checking the checkboxes in the department list on the right side of this page. The default department is EVERYONE. More details about the Department will be discussed in the next section (page 46).

Advanced Information

This tab contains more optional fields for the employees for payroll purpose, including Martial Status, Birthday, Bank Name, Bank Account, Date Joined, Probation, Date Left and Address. These optional fields, if used, will also be synchronized across the device and the *iGuardPayroll* cloud service.

Press the **Save** button at the bottom to save the change.

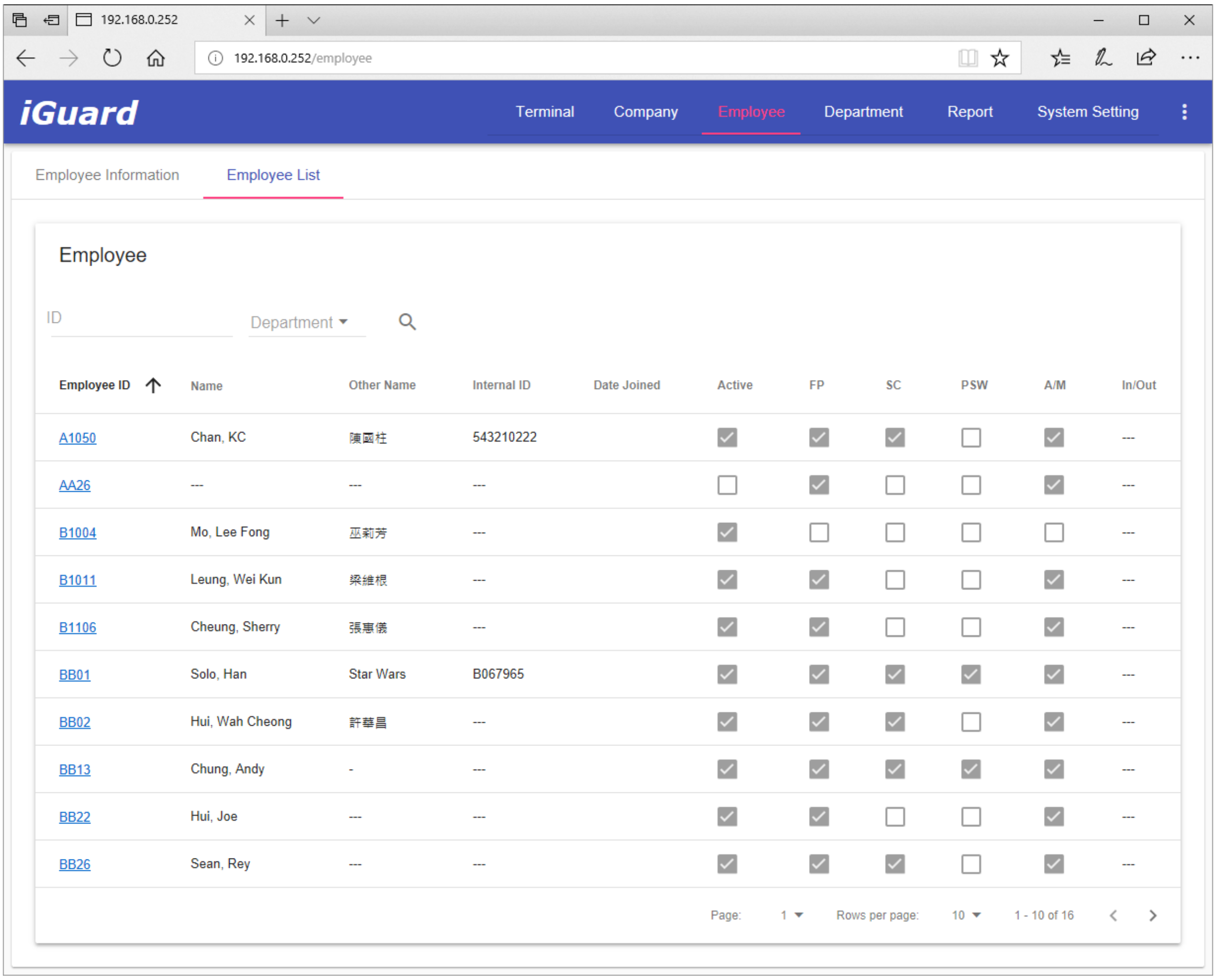
Press the **Delete** button to delete this particular employee.

Note: Once the user ID is deleted, all the information associated with the user, including the fingerprint data, name, and the access right, will also be permanently deleted. The user must be re-registered to regain access rights. However, access log data will be retained.

Press the **New** button at the top of the left hand column to add new employees.

Employee List

The *Employee List* shows all the registered employees as shown below:



Employee

ID

Department ▾

Employee ID ↑	Name	Other Name	Internal ID	Date Joined	Active	FP	SC	PSW	A/M	In/Out
A1050	Chan, KC	陳國柱	543210222		☑	☑	☑	□	☑	---
AA26	---	---	---		□	☑	□	□	☑	---
B1004	Mo, Lee Fong	巫莉芳	---		☑	□	□	□	□	---
B1011	Leung, Wei Kun	梁維根	---		☑	☑	□	□	☑	---
B1106	Cheung, Sherry	張惠儀	---		☑	☑	□	□	☑	---
BB01	Solo, Han	Star Wars	B067965		☑	☑	☑	☑	☑	---
BB02	Hui, Wah Cheong	許華昌	---		☑	☑	☑	□	☑	---
BB13	Chung, Andy	-	---		☑	☑	☑	☑	☑	---
BB22	Hui, Joe	---	---		☑	☑	□	□	☑	---
BB26	Sean, Rey	---	---		☑	☑	☑	□	☑	---

Page: 1 ▾ Rows per page: 10 ▾ 1 - 10 of 16 ‹ ›

There are five columns on the right side of the list with *checkboxes* (i.e., ON / OFF) indicators. These are: -

- The ***Active*** Indicator indicates that the employee is in Active status (i.e., not suspended).

- The ***FP*** (Fingerprint) indicator shows whether the user has registered his fingerprint image, and he can use fingerprint for authentication.

- The ***SC*** (Smartcard) indicator shows that a Smartcard has been issued to the user.

- The ***PSW*** (Password) indicator shows a Personal Password has been assigned to the user. Personal Password is optionally assigned to each individual user using **Func 1** in the function menu as discussed previously, or can be assigned using the browser in the user setup page, which will be discussed later in this section.

- The ***AM*** (Auto-Match) indicator indicates that the optional auto-match feature is enabled for the particular user. If enabled, during fingerprint authentication, the user can simply lift the shutter and place the finger on the sensor for authentication without the need to enter his ID first.

The last column is the *In/Out monitor* for each employee, which shows the time and the access status of the corresponding last access entry. The information is reset daily at midnight.

The text boxes at the top allow you to search by ID and/or filter these results by Department.

Scroll down to the bottom of the right panel, and the three buttons, Activate, Deactivate & Delete, will appear. One can Activate, Deactivate & Delete a single employee or a group of employees by first checking the checkbox and then pressing the corresponding button.

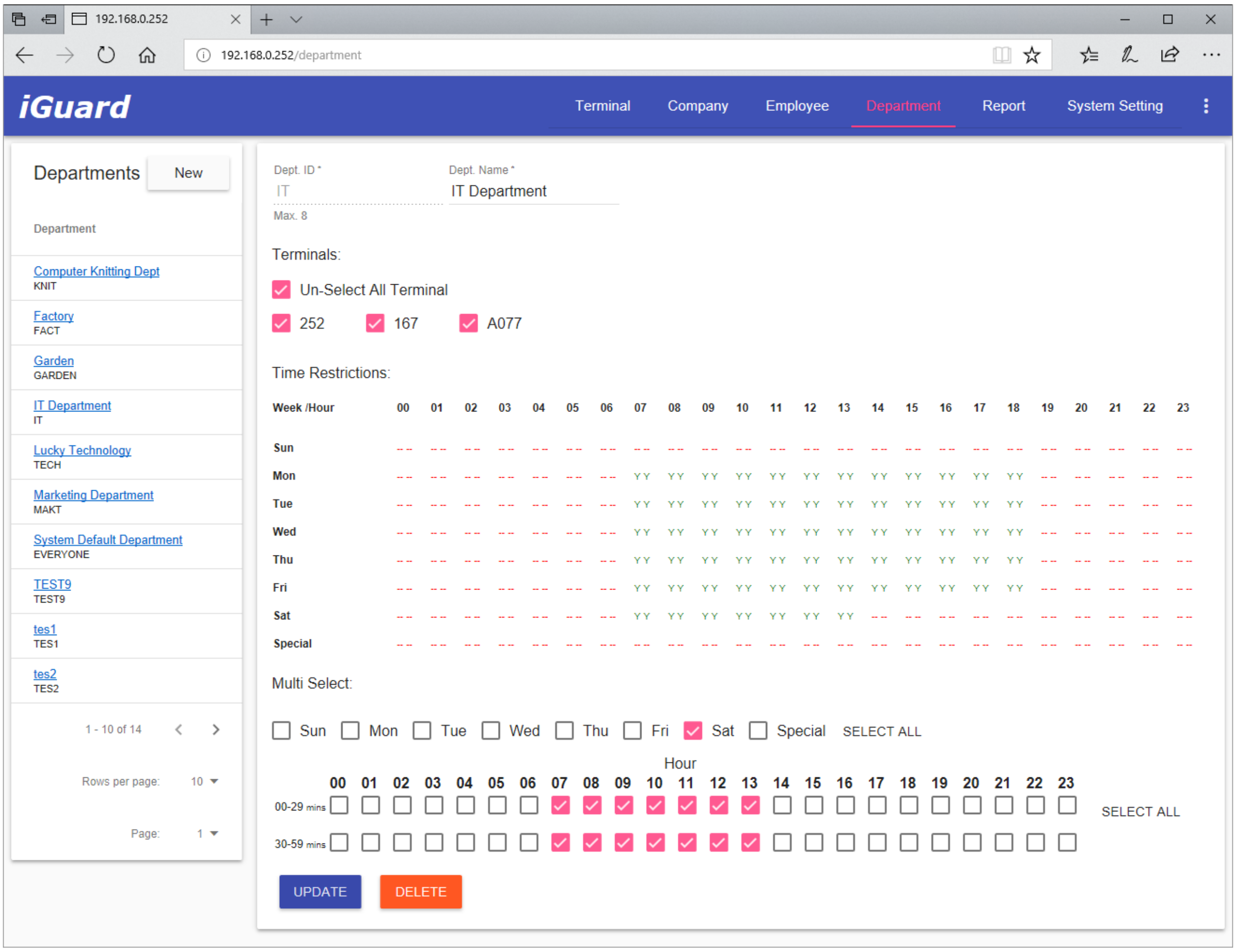
Press the employee ID hyperlink to edit the information of each employee.

Department

Prior to adding employees to the iGuard unit, it is a good idea to establish departments. For smaller companies, this may not be as applicable, but departments are helpful for establishing permission to individual iGuard units, and access times for groups of employees.

In a typical setting, the Executive and Accounting departments may be the only employees with access to the accounting file room during normal business hours, and your Tech department might contain anyone authorized to enter the server room at any time, while everyone in the company can come and go through the front door at any time except weekends and company holidays.

The Department page is shown below:



Departments New

Department
Computer Knitting Dept KNIT
Factory FACT
Garden GARDEN
IT Department IT
Lucky Technology TECH
Marketing Department MAKT
System Default Department EVERYONE
TEST9 TEST9
tes1 TES1
tes2 TES2

1 - 10 of 14

Rows per page: 10

Page: 1

Dept. ID * IT
Max. 8

Dept. Name * IT Department

Terminals:

☑ Un-Select All Terminal

☑ 252 ☑ 167 ☑ A077

Time Restrictions:

Week /Hour	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sun	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Mon	--	--	--	--	--	--	--	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	--	--	--	--	--
Tue	--	--	--	--	--	--	--	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	--	--	--	--	--
Wed	--	--	--	--	--	--	--	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	--	--	--	--	--
Thu	--	--	--	--	--	--	--	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	--	--	--	--	--
Fri	--	--	--	--	--	--	--	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	--	--	--	--	--
Sat	--	--	--	--	--	--	--	YY	YY	YY	YY	YY	YY	YY	--	--	--	--	--	--	--	--	--	--
Special	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Multi Select:

☐ Sun ☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☑ Sat ☐ Special SELECT ALL

Hour

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	
00-29 mins	☐	☐	☐	☐	☐	☐	☐	☑	☑	☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	SELECT ALL
30-59 mins	☐	☐	☐	☐	☐	☐	☐	☑	☑	☑	☑	☑	☑	☑	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	

UPDATE DELETE

The Left Column shows a complete list of the departments. Each department is represented by its Department name (in blue hyperlink) and the department ID. Click on the link will show the details of the department. You can edit the Department Name, the authorized Terminals, and the authored period of time in this page.

Press the **Update** button to update the changes.

Press the **Delete** button to delete the department.

Press the **New** button at the upper left column to add a new department.

In the screen shot example above, the authorized time period for the *IT Department* is from 7:00am am to 6:59 pm, Monday to Friday, and from 7:00am to 13:59pm on Saturday.

Note: All the members of this department can only access the unit during this authorized period.

The upper part of the page, *Terminals*, specifies the "doors" to which this department has the access rights. This is only applicable when multiple iGuards are connected together and form a Master / Slave network. If there is only one iGuard or the iGuard is not connected to any Master / Slave network, there will only be one item in this "*Terminals*" section, which is the Terminal ID of the iGuard itself.

Check the checkbox "*Any Terminal*" to allow the department members to access any iGuard unit in the network.

The authorized time of a particular day, Monday for example, can be edited by clicking on the *Monday* button, and the following web page will appear.

The *"System Default Department" (ID: EVERYONE)* is the default department and it cannot be deleted. By default, each new employee created will automatically be added to the "*EVERYONE*" department.

The maximum length of the Department ID is 8 characters.

Although unlimited number of departments can be assigned, it is suggested that the number not to exceed 100 for better maintenance.

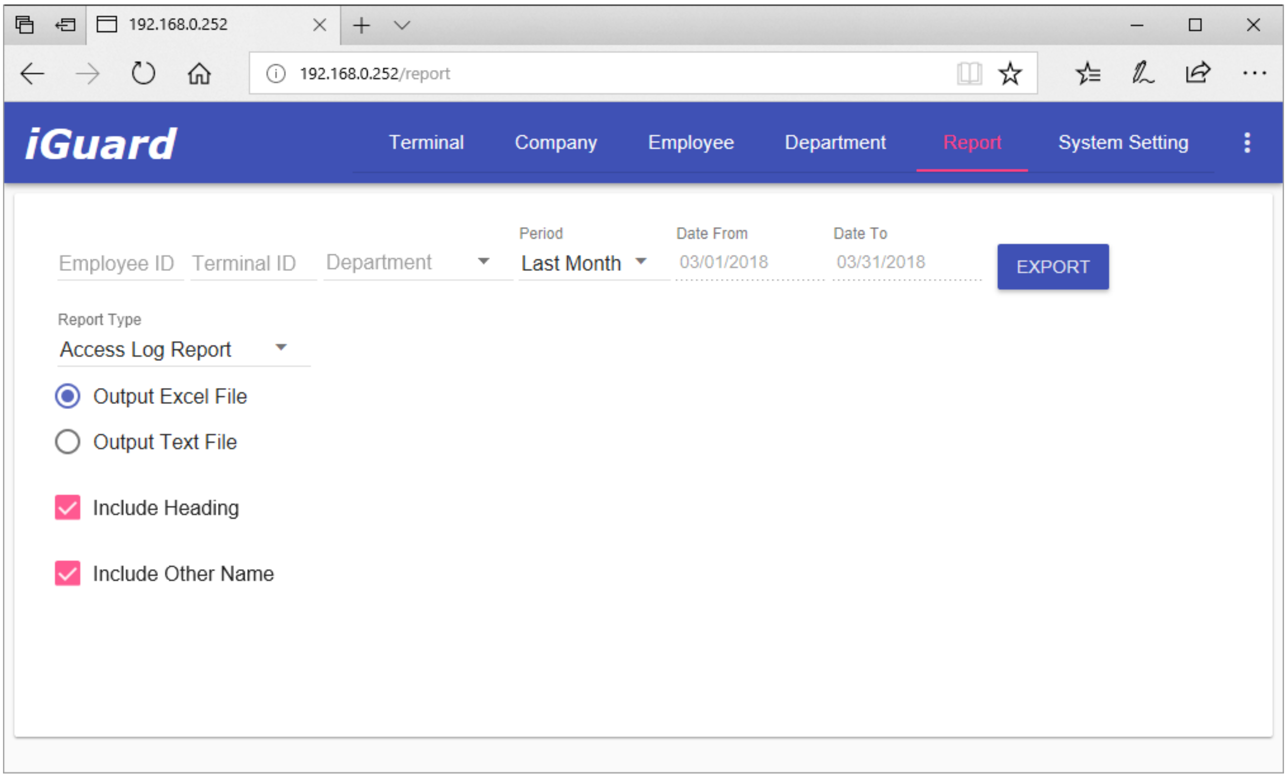
Report

Use this tab to export the following reports in Microsoft Excel (csv) format or plain text format.

Currently the following reports are supported:

- Access Log Report
- Attendance Report
- Daily In / Out Report

The following is a screen sample of this Report page:



Employee ID

Terminal ID

Department

Period: Last Month

Date From: 03/01/2018

Date To: 03/31/2018

EXPORT

Report Type: Access Log Report

● Output Excel File

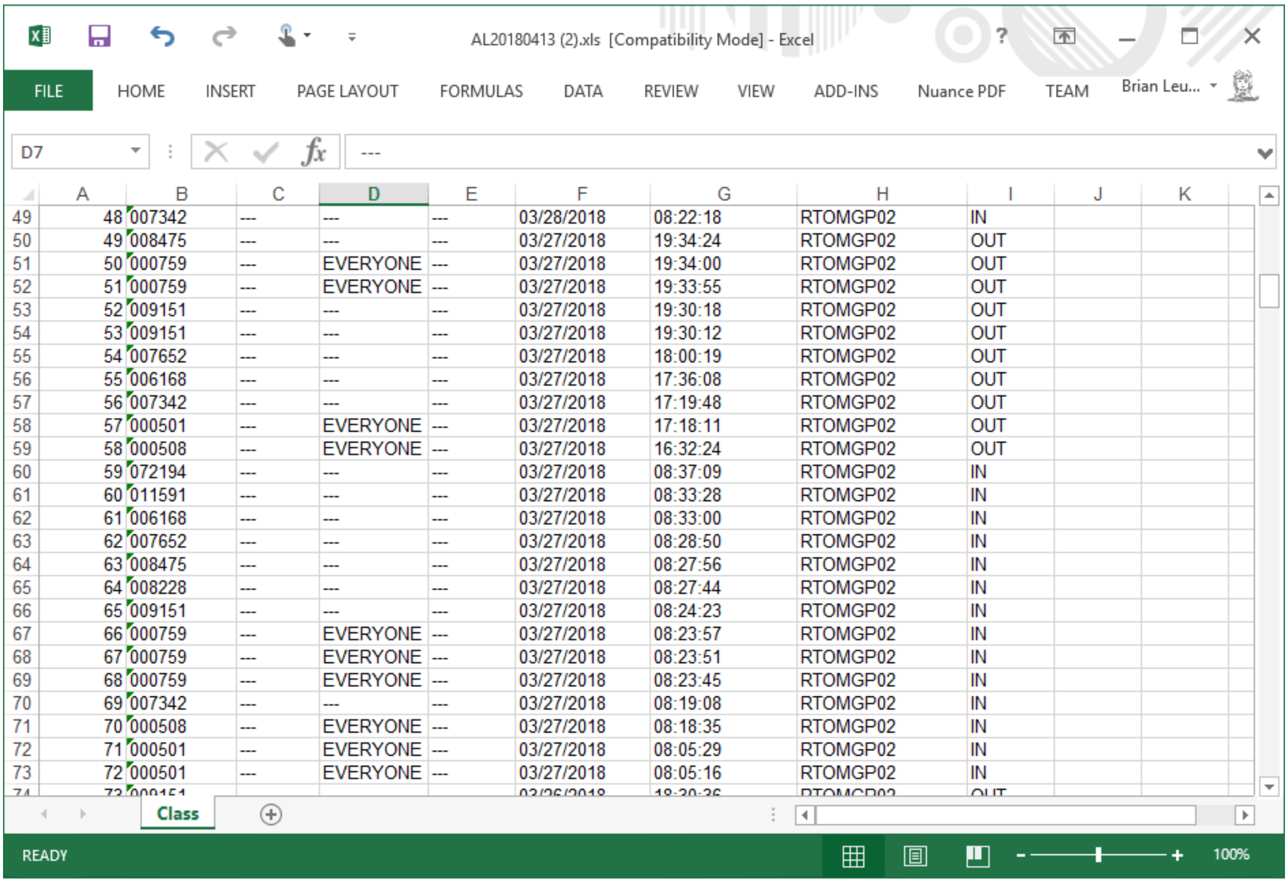
○ Output Text File

☑ Include Heading

☑ Include Other Name

Again, you can specify the Employee ID, Terminal ID, Department, and the Date Range to filter the output.

The following is a sample Excel output (in ‘csv’ format) of an Access Log Report:



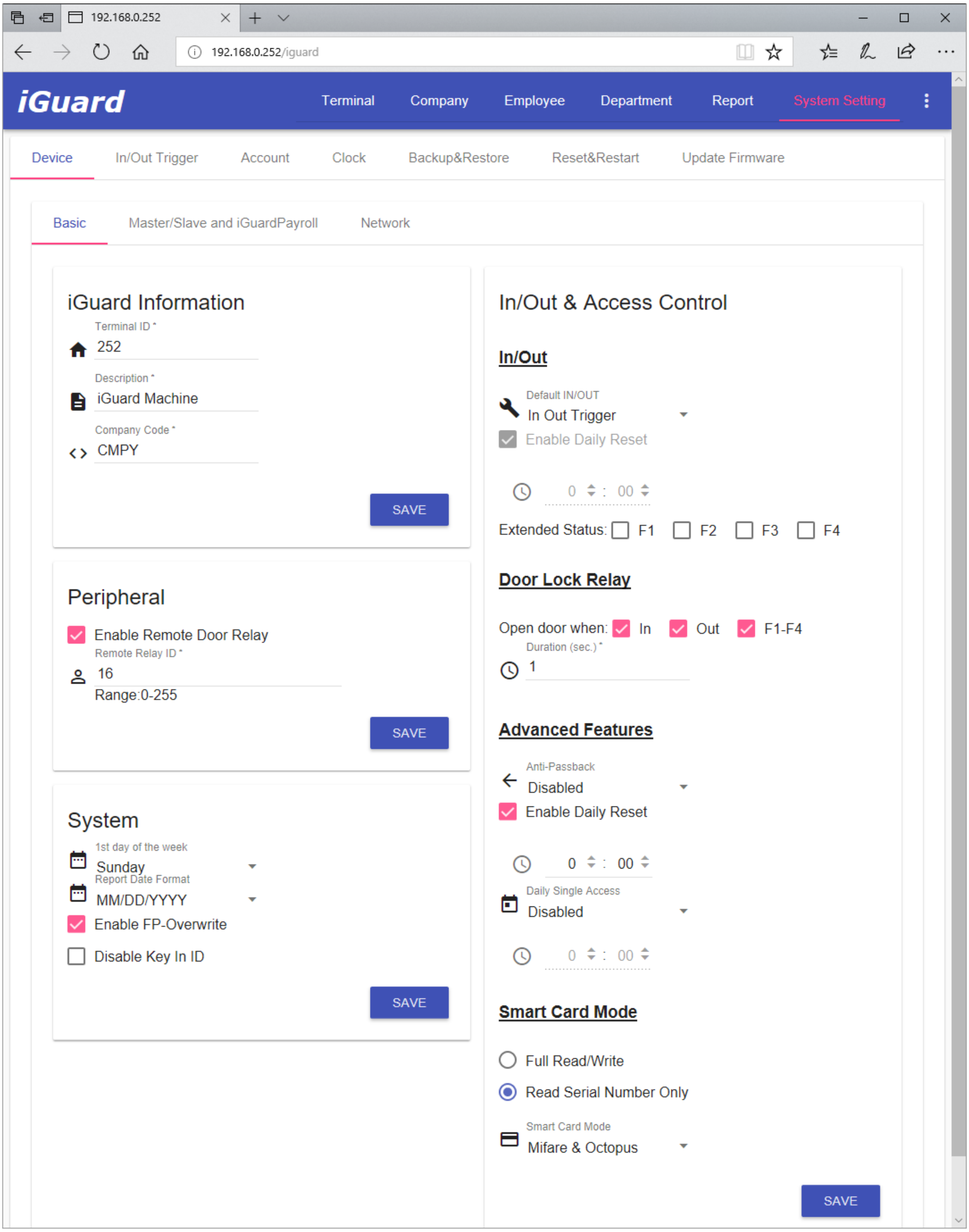
	A	B	C	D	E	F	G	H	I
49	48	007342	---	---	---	03/28/2018	08:22:18	RTOMGP02	IN
50	49	008475	---	---	---	03/27/2018	19:34:24	RTOMGP02	OUT
51	50	000759	---	EVERYONE	---	03/27/2018	19:34:00	RTOMGP02	OUT
52	51	000759	---	EVERYONE	---	03/27/2018	19:33:55	RTOMGP02	OUT
53	52	009151	---	---	---	03/27/2018	19:30:18	RTOMGP02	OUT
54	53	009151	---	---	---	03/27/2018	19:30:12	RTOMGP02	OUT
55	54	007652	---	---	---	03/27/2018	18:00:19	RTOMGP02	OUT
56	55	006168	---	---	---	03/27/2018	17:36:08	RTOMGP02	OUT
57	56	007342	---	---	---	03/27/2018	17:19:48	RTOMGP02	OUT
58	57	000501	---	EVERYONE	---	03/27/2018	17:18:11	RTOMGP02	OUT
59	58	000508	---	EVERYONE	---	03/27/2018	16:32:24	RTOMGP02	OUT
60	59	072194	---	---	---	03/27/2018	08:37:09	RTOMGP02	IN
61	60	011591	---	---	---	03/27/2018	08:33:28	RTOMGP02	IN
62	61	006168	---	---	---	03/27/2018	08:33:00	RTOMGP02	IN
63	62	007652	---	---	---	03/27/2018	08:28:50	RTOMGP02	IN
64	63	008475	---	---	---	03/27/2018	08:27:56	RTOMGP02	IN
65	64	008228	---	---	---	03/27/2018	08:27:44	RTOMGP02	IN
66	65	009151	---	---	---	03/27/2018	08:24:23	RTOMGP02	IN
67	66	000759	---	EVERYONE	---	03/27/2018	08:23:57	RTOMGP02	IN
68	67	000759	---	EVERYONE	---	03/27/2018	08:23:51	RTOMGP02	IN
69	68	000759	---	EVERYONE	---	03/27/2018	08:23:45	RTOMGP02	IN
70	69	007342	---	---	---	03/27/2018	08:19:08	RTOMGP02	IN
71	70	000508	---	EVERYONE	---	03/27/2018	08:18:35	RTOMGP02	IN
72	71	000501	---	EVERYONE	---	03/27/2018	08:05:29	RTOMGP02	IN
73	72	000501	---	EVERYONE	---	03/27/2018	08:05:16	RTOMGP02	IN

System Setting

This is used to system configuration and maintenance.

Device

Use this tab to configure the system as shown below:



iGuard Information

Terminal ID * 252

Description * iGuard Machine

Company Code * CMPY

SAVE

Peripheral

☑ Enable Remote Door Relay

Remote Relay ID * 16

Range:0-255

SAVE

System

1st day of the week: Sunday

Report Date Format: MM/DD/YYYY

☑ Enable FP-Overwrite

□ Disable Key In ID

SAVE

In/Out & Access Control

In/Out

Default IN/OUT: In Out Trigger

☑ Enable Daily Reset

0 : 00

Extended Status: □ F1 □ F2 □ F3 □ F4

Door Lock Relay

Open door when: ☑ In ☑ Out ☑ F1-F4

Duration (sec.) * 1

Advanced Features

Anti-Passback: Disabled

☑ Enable Daily Reset

0 : 00

Daily Single Access: Disabled

0 : 00

Smart Card Mode

○ Full Read/Write

● Read Serial Number Only

Smart Card Mode: Mifare & Octopus

SAVE

Basic – iGuard Information

Terminal ID – Assign an ID to the unit. In a Master / Slave configuration, this Terminal ID is used to identify each slave unit in the network. Identical ID can be assigned to different iGuards. However, it is suggested to assign unique ID to each iGuard in a Master / Slave configuration, to avoid confusion when assigning departments' access right, in which the Terminal ID is used to identify which iGuard in the network is accessible by the department's members.

Description – Assign a descriptive name to the unit, for displaying in the "Terminal List" page.

Company Code – This is applicable for Smart Card operation only, when the *Smart Card Mode* is set to "Full Read/Write" mode. This Code is a 4-character string that will be written to the smartcards issued by the unit. When reading the card, iGuard will first compare the smartcard's code against the device's code. If they do not match, iGuard will just simply ignore the card.

The default is "CMPY".

The *Smart Card Mode* can be configured in the same setup page, and will be discussed later (page 54).

Warning: This value must be set prior to issuing any smartcard, and must not be changed afterwards. Otherwise, all previously issued smartcards will be ignored.

Basic – Peripheral

This is for setting up the optional *Remote Door Relay*, which is a small device for controlling the electric door strike.

Normally, the electric door strike is connected directly to the built-in door relay of the device. For higher security purpose, this Remote Door Relay can be used instead of the built-in one to control the door strike, to avoid the possible intruder break-in by opening the iGuard and directly shorting the door strike wires.

More details will be discussed in the Appendix (page 67).

Enable Remote Door Relay – Enable this if the optional Remote Door Relay is available.

Remote Relay ID – This number must match the 8-bit jumper block setting located on Remote Door Relay device.

Basic – System

1st day of the week – Use this to change the first day of the week from the default Sunday to others (useful for some Muslim countries and Hispanic).

Report Date Format – Select the desired date format from the list. Available date formats are MM/DD/YYYY, MM-DD-YYYY, DD/MM/YYYY and more.

Enable FP (Fingerprint) Overwrite – By default, during the fingerprint enrollment procedure, the newly submitted fingerprint information will overwrite any existing one after confirmed by the user. This is to disable the overwrite capability.

Once the fingerprint is enrolled for a user, the fingerprint information cannot be changed in any way later on. The main purpose for this feature is to avoid accidentally overwriting one's fingerprint information if a wrong user ID is entered during fingerprint enrollment.

If enabled, the administrator must delete a user and then re-create the user in order to re-enroll the user's fingerprint.

The default of this setting is true.

Disable 'Key-In' ID – This is to disable the ability to use the keypad to enter user ID. This achieves a higher security level. If this option is set, the user must use his Smartcard or use the AutoMatch approach for verification, because he can no longer use the keypad to enter his ID for verification.

Basic – In/Out & Access Control

In/Out – Default IN/OUT -- This is to define the default user access status, i.e., how the iGuard will log each clock event. iGuard assigns the access status to each access log entry, such as IN & OUT. The default access status is shown on the iGuard LCD display in Standby Mode. The default available options are *Always IN*, *Always OUT*, *In/Out Trigger*, *Smart In/Out & Auto In/Out*.

If *Extended Status* is enabled, the corresponding status will be added to the options above. For example, if F1 & F2 are enabled, the two corresponding optional status will be added: *Always F1* & *Always F2*.

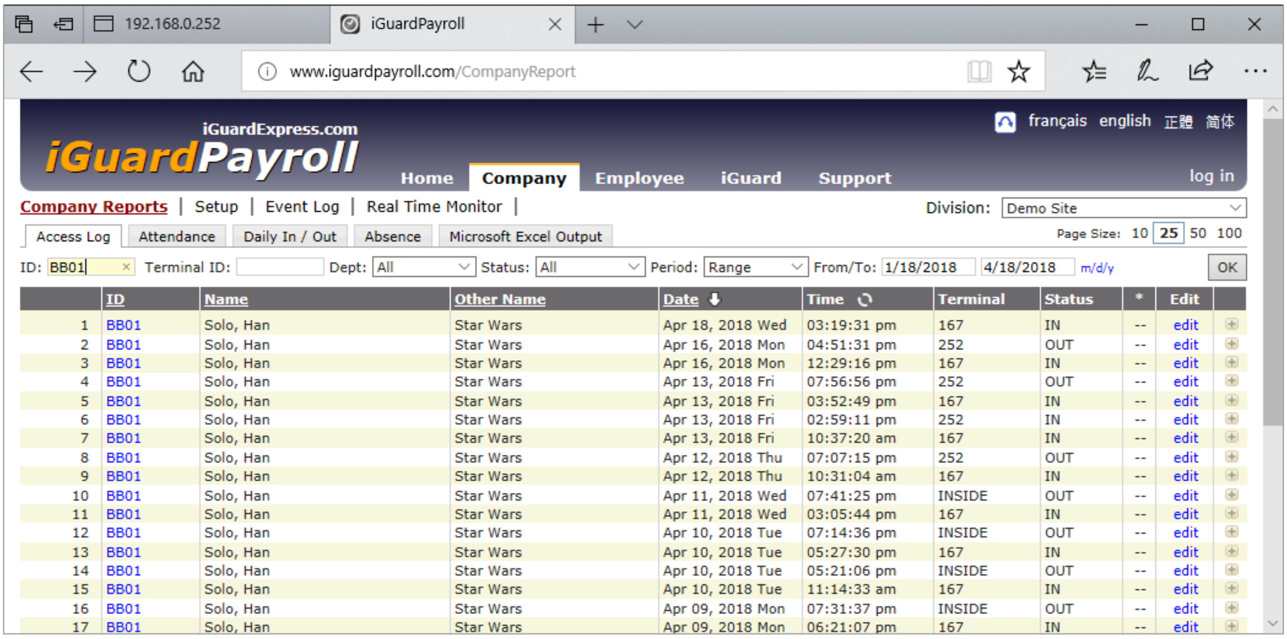
In the '*IN/OUT Trigger'* option, the default IN/OUT status follows the settings configured in the *"In/Out Trigger"* page, which will be discussed later in this section. In this option, one can still change the default access status in an ad hoc basis by pressing the **Backspace** key on the keypad a few times to toggle the IN/OUT status, until the desired access status is shown on the LCD display.

The *'Auto In/Out'* option allows the system to automatically assign the in/out status based on the employee's previous access log status. For example, if the previous status is IN, the new access log status will be OUT. Similarly, if the last status is OUT, the new status would be IN. This feature works with the next setting *'Enabled Daily Reset'*, which is to be discussed below.

And similar to the *'In/Out Trigger'* option, one can press the **Backspace** key to override the assigned status before clocking in/out the machine.

The *'Smart In/Out'* option only works with the iGuardPayroll[8] Cloud Service. In iGuardPayroll, each employee can be assigned a working roster / schedule, and the status of each access log record will be intelligently assigned by iGuardPayroll based on the log time according to the roster as follows:

[8] For more information, please visit www.iguardpayroll.com



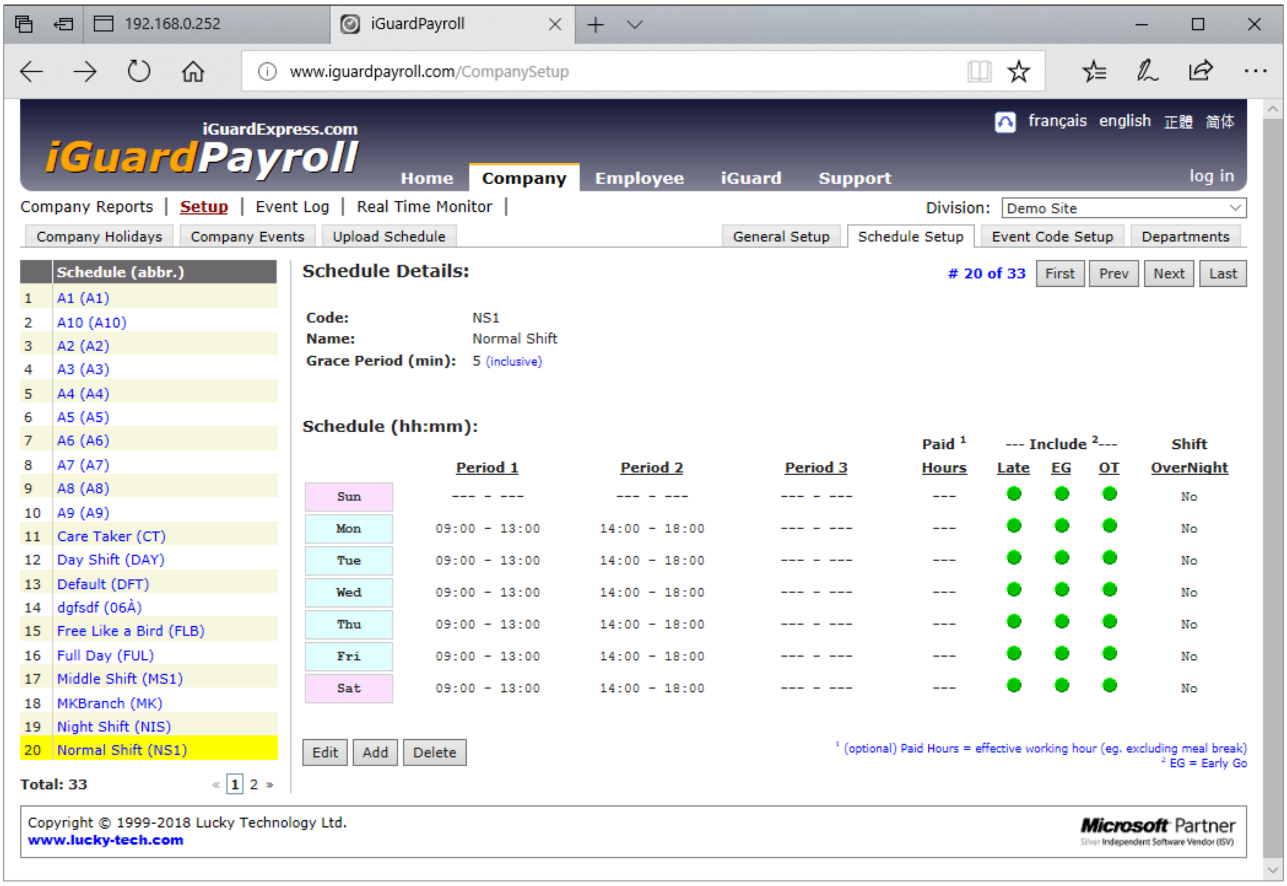
Division: Demo Site

Page Size: 10 25 50 100

ID: BB01 Terminal ID: Dept: All Status: All Period: Range From/To: 1/18/2018 4/18/2018 m/d/y

	ID	Name	Other Name	Date	Time	Terminal	Status	*	Edit	
1	BB01	Solo, Han	Star Wars	Apr 18, 2018 Wed	03:19:31 pm	167	IN	--	edit	⊞
2	BB01	Solo, Han	Star Wars	Apr 16, 2018 Mon	04:51:31 pm	252	OUT	--	edit	⊞
3	BB01	Solo, Han	Star Wars	Apr 16, 2018 Mon	12:29:16 pm	167	IN	--	edit	⊞
4	BB01	Solo, Han	Star Wars	Apr 13, 2018 Fri	07:56:56 pm	252	OUT	--	edit	⊞
5	BB01	Solo, Han	Star Wars	Apr 13, 2018 Fri	03:52:49 pm	167	IN	--	edit	⊞
6	BB01	Solo, Han	Star Wars	Apr 13, 2018 Fri	02:59:11 pm	252	IN	--	edit	⊞
7	BB01	Solo, Han	Star Wars	Apr 13, 2018 Fri	10:37:20 am	167	IN	--	edit	⊞
8	BB01	Solo, Han	Star Wars	Apr 12, 2018 Thu	07:07:15 pm	252	OUT	--	edit	⊞
9	BB01	Solo, Han	Star Wars	Apr 12, 2018 Thu	10:31:04 am	167	IN	--	edit	⊞
10	BB01	Solo, Han	Star Wars	Apr 11, 2018 Wed	07:41:25 pm	INSIDE	OUT	--	edit	⊞
11	BB01	Solo, Han	Star Wars	Apr 11, 2018 Wed	03:05:44 pm	167	IN	--	edit	⊞
12	BB01	Solo, Han	Star Wars	Apr 10, 2018 Tue	07:14:36 pm	INSIDE	OUT	--	edit	⊞
13	BB01	Solo, Han	Star Wars	Apr 10, 2018 Tue	05:27:30 pm	167	IN	--	edit	⊞
14	BB01	Solo, Han	Star Wars	Apr 10, 2018 Tue	05:21:06 pm	INSIDE	OUT	--	edit	⊞
15	BB01	Solo, Han	Star Wars	Apr 10, 2018 Tue	11:14:33 am	167	IN	--	edit	⊞
16	BB01	Solo, Han	Star Wars	Apr 09, 2018 Mon	07:31:37 pm	INSIDE	OUT	--	edit	⊞
17	BB01	Solo, Han	Star Wars	Apr 09, 2018 Mon	06:21:07 pm	167	IN	--	edit	⊞

And the following is a sample screen shot showing how a schedule is assigned:



Division: Demo Site

	Schedule (abbr.)
1	A1 (A1)
2	A10 (A10)
3	A2 (A2)
4	A3 (A3)
5	A4 (A4)
6	A5 (A5)
7	A6 (A6)
8	A7 (A7)
9	A8 (A8)
10	A9 (A9)
11	Care Taker (CT)
12	Day Shift (DAY)
13	Default (DFT)
14	dgfsdf (06À)
15	Free Like a Bird (FLB)
16	Full Day (FUL)
17	Middle Shift (MS1)
18	MKBranch (MK)
19	Night Shift (NIS)
20	Normal Shift (NS1)

Total: 33 « 1 2 »

Schedule Details: # 20 of 33

Code: NS1
Name: Normal Shift
Grace Period (min): 5 (inclusive)

Schedule (hh:mm):

	Period 1	Period 2	Period 3	Paid [1] Hours	--- Include [2]--- Late	 EG	 OT	Shift OverNight
Sun	--- - ---	--- - ---	--- - ---	---	●	●	●	No
Mon	09:00 - 13:00	14:00 - 18:00	--- - ---	---	●	●	●	No
Tue	09:00 - 13:00	14:00 - 18:00	--- - ---	---	●	●	●	No
Wed	09:00 - 13:00	14:00 - 18:00	--- - ---	---	●	●	●	No
Thu	09:00 - 13:00	14:00 - 18:00	--- - ---	---	●	●	●	No
Fri	09:00 - 13:00	14:00 - 18:00	--- - ---	---	●	●	●	No
Sat	09:00 - 13:00	14:00 - 18:00	--- - ---	---	●	●	●	No

[1] (optional) Paid Hours = effective working hour (eg. excluding meal break)
[2] EG = Early Go

Copyright © 1999-2018 Lucky Technology Ltd.
www.lucky-tech.com

<u>In/Out – Enable Daily Reset</u> – this setting is for *'Auto In/Out'* only (discussed above). If this is enabled, the system will exclude any access log 'before' the daily reset time as a previous record, allowing the system to reset the in/out status every day.

For example, if *'Auto In/Out'* is selected as the default in/out, and an employee forgot to clock *out* when she left the office, and when she clocks in the next day, the system will assign the status of the new access log as IN.

In/Out – Extended Status -- Four additional access statuses, F1 to F4, are available as well as the normal IN and OUT status. Enable any one or all of these four additional access statuses by checking the corresponding checkboxes.

As an example, assign F1 as *Lunch Out*, and F2 *as Lunch In*, so the employees can use F1 when they are out for lunch, and use F2 when they are back from lunch.

Door Lock Relay – this is to configure if the built-in door relay will be switched on for the corresponding access log status. This is also applicable to the optional Remote Door Relay unit (which will be discussed in the Appendix).

For example, if the option *'Open door when IN'* is checked, the built-in door relay will be switched on for all successful clock-in accesses. Likewise, if the option for *OUT* is checked, the door relay will be switched on for the clock-out accesses.

Note: This option is useful if the device is installed outside of the main door of the premises, and the device is used for both access control and time keeping purposes. By disabling this option, the door will not open if someone clocks-out from the device when leaving the place.

The *Duration (sec)* entry is used to specify the duration (in second) of the door relay when it is switched on. The default is 3 seconds. Set this to a larger value if the iGuard is installed immediately next to the door, and the user may take a few seconds to reach the door after being authenticated.

Advanced Features – Anti-Passback -- This option is for avoiding two consecutive records with the same in/out status, i.e., to make sure that one must clock-out first before he can clockin again.

This is useful in Access Control applications, e.g., computer server room, to keep track of how long one had stayed in the room as he must clock-out when he leaves the room, otherwise he won't be able to clock-in and enter the room again.

It is also useful for Time Attendance purpose in making sure that no one would clock-in twice in a row by mistake, which is important for the payroll for example. You can further specify the order to include the lunch break by selecting the 2nd option IN-(F1-F2)-OUT (selectable at the pull-down menu under this section). In this case, one must either clock-in or clock-F2 first (e.g., return from lunch) before he can clock-out at the end of the day.

This Anti-PassBack option is a systemwise option, i.e., you only need to set this up in the Master unit and it applies to all its slave units automatically. In other words, if one clocks-in at one unit, he cannot clock-in again at any other unit until he clocks-out at any one of these units first.

Check the *'Enable Daily Reset'* option and specify the daily reset time to clear all the Anti-Passback status everyday at the specific time. To illustration how this option works, if an employee forgot to clock-out one day, she will not be able to clock-in the next day. By enabling this option and clearing the Anti-Passback status at 12:00 midnight for example, the user can clock-in again the next day.

Advanced Features – Daily Single Access - This is to limit the user to access the iGuard unit only once everyday, i.e., one cannot enter the same place twice in one day.

This is mainly for some access control applications, like the company canteen for example, to make sure that no one can eat lunch twice in a day.

There are three different options: This Terminal Only, Group, and System. The first one is for setting up each individual unit.

The second one is for setting a group of units, e.g., if there are multiple units for the canteen, you can set all these units to "Group", and the user in/out status will be shared among this group.

Similarly, the "System" option is used to apply the setting to all units that also have selected this "System" option.

Unlike the Anti-PassBack option, this Daily Single Access option is not a system option, i.e., you must set this up in each unit individually, and it won't affect the other units.

Similar to the Anti-Passback Daily Reset Time, you can also specify a time so this feature will clear the corresponding status everyday at that specific time.

Smart Card Mode – There are two options in this mode: *'Full Read/Write'* mode and *'Read Serial Number Only'* mode.

Full Read/Write mode: In this mode, partial information of each employee is written and stored in his own smartcard, including the employee ID, Name, Personal Password and Fingerprint Data. This allows the system to *optionally* clear the employee's fingerprint data from the internal storage, and the smartcard would be the only media that contains the fingerprint information, thus the privacy of the employee can be better protected.

During verification, iGuard will read all the contents of the Smartcard first, and then it will compare the fingerprint information saved in the Smartcard against the submitted fingerprint image for authentication.

Please refer to the smartcard chart on page 11 for a list of supported smartcard types for this mode.

Read Serial Number Only mode: In this mode, iGuard would only read the serial number of the smartcard. It would neither read any data stored at the smartcard, nor write any data to it.

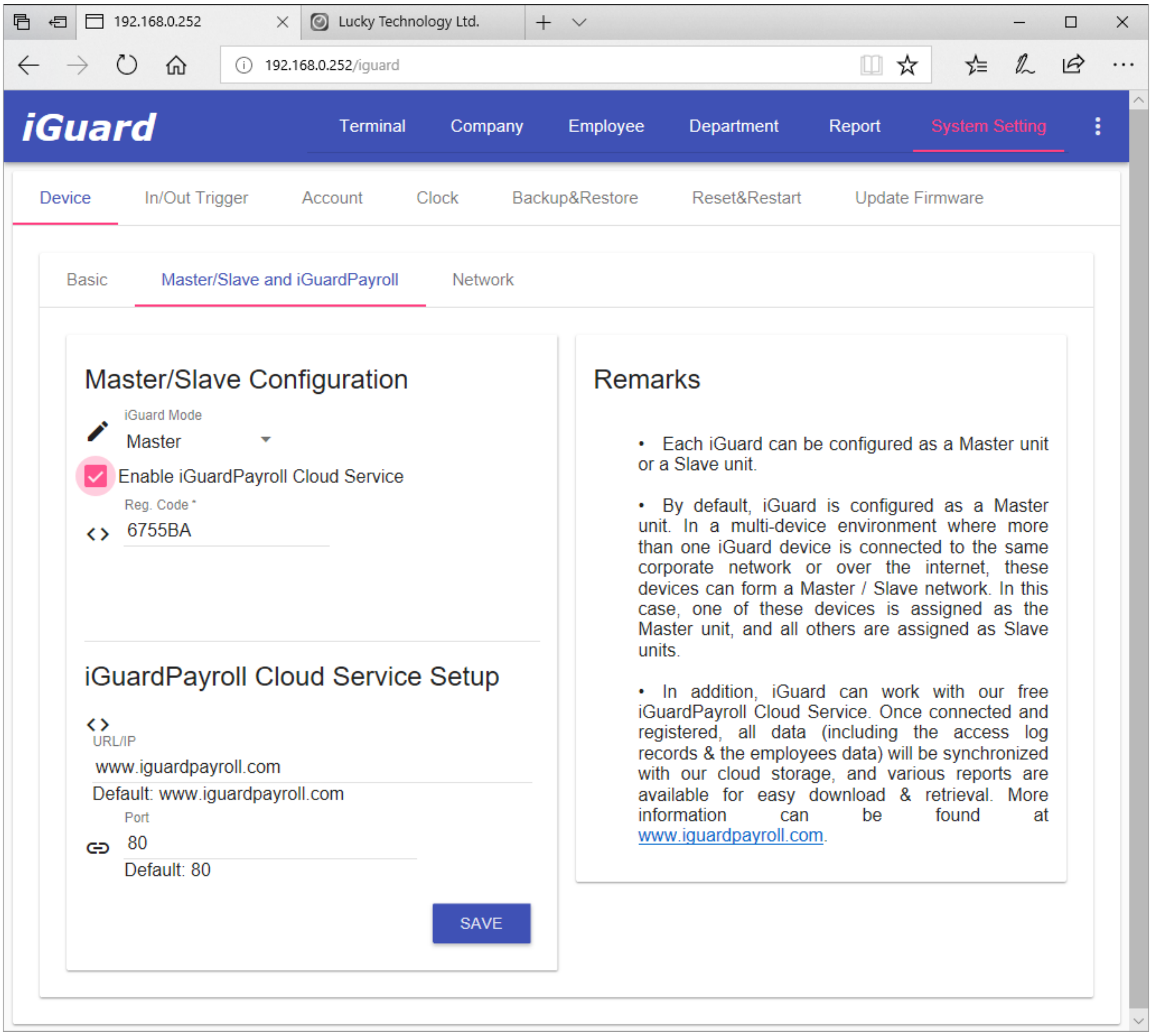
During verification, iGuard will read the serial number of the smartcard, and then search for the employee from the internal storeage based on this unique serial number. If found, the information will be retrieved and compared against the fingerprint image and other data entered for authentication.

Using this mode, the company no longer needs to provide smartcards to its employees, since they can use their own smartcards for verification. Since iGuard supports most of the smartcard commonly available, including the popular transportation card Octopus in Hong Kong for instance, it would be very convenient for both companies and employees in this mode.

Please refer to page 10 for more information on Smart Card types.

Master / Slave Configuration and iGuardPayroll

Use this page to configure the iGuard as either a Master or Slave unit[9], and to connect the device to the iGuardPayroll cloud service.



Master/Slave Configuration

iGuard Mode: Master

☑ Enable iGuardPayroll Cloud Service

Reg. Code *: 6755BA

iGuardPayroll Cloud Service Setup

URL/IP: www.iguardpayroll.com

Default: www.iguardpayroll.com

Port: 80

Default: 80

Remarks

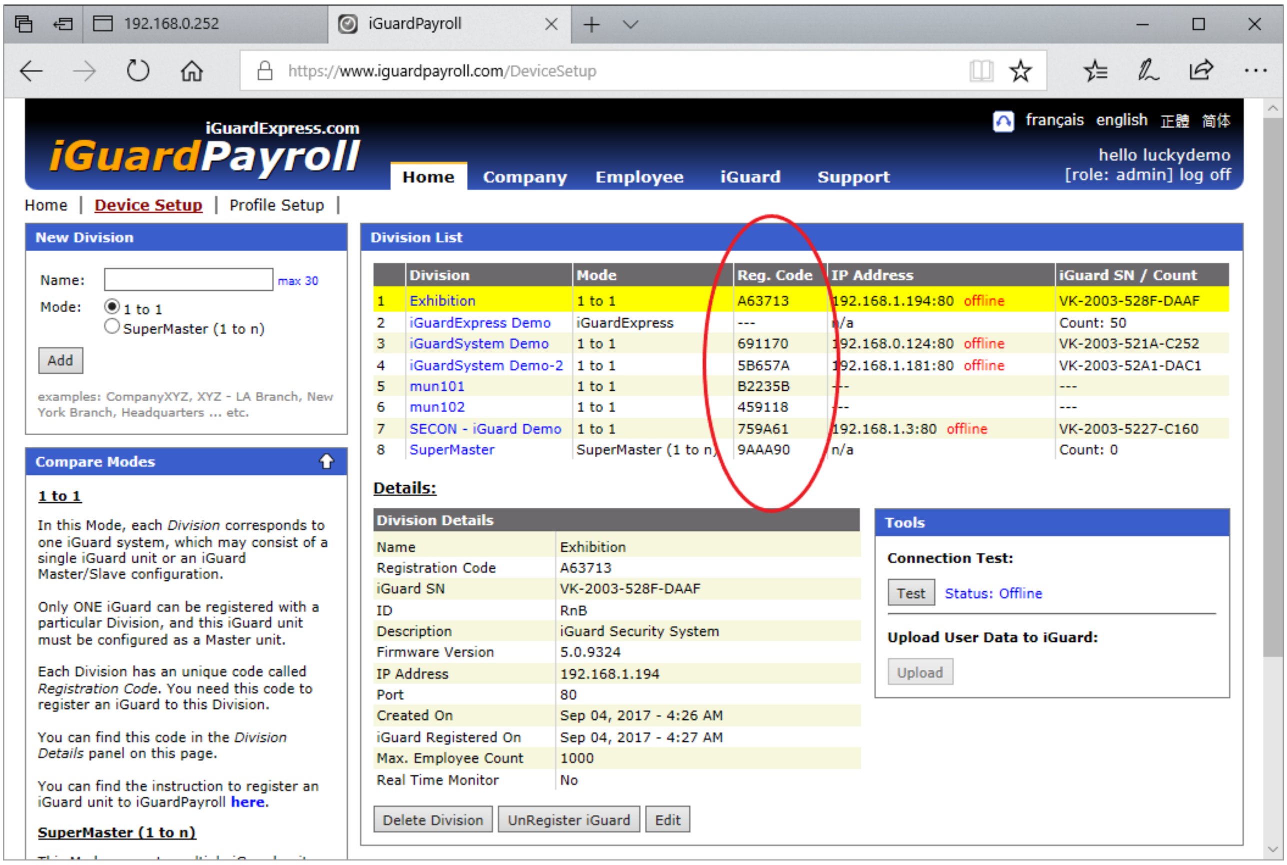
- Each iGuard can be configured as a Master unit or a Slave unit.
- By default, iGuard is configured as a Master unit. In a multi-device environment where more than one iGuard device is connected to the same corporate network or over the internet, these devices can form a Master / Slave network. In this case, one of these devices is assigned as the Master unit, and all others are assigned as Slave units.
- In addition, iGuard can work with our free iGuardPayroll Cloud Service. Once connected and registered, all data (including the access log records & the employees data) will be synchronized with our cloud storage, and various reports are available for easy download & retrieval. More information can be found at www.iguardpayroll.com.

Master/Slave Configuration – use this page to configure iGuard as either a Master or Slave unit.

Master Mode: In Master Mode, you can select the "*Enable iGuardPayroll Cloud Service"* to connect to the service. A master unit can be connected to iGuardPayroll cloud services for storing all the employee information and access logs for free.

If iGuardPayroll is enabled, the device must be associated with an iGuardPayroll user account, which has a unique registration code. Enter the registration code here to notify iGuardPayroll the user account the iGuard unit belongs to. The registration code is a six-digit code and can be found in iGuardPayroll's *'Device Setup'* page as follows:

[9] Please refer to the section "Master / Slave Mode" on page 19 for more detail.



New Division

Name: max 30

Mode: ● 1 to 1 ○ SuperMaster (1 to n)

Add

examples: CompanyXYZ, XYZ - LA Branch, New York Branch, Headquarters ... etc.

Compare Modes

1 to 1

In this Mode, each *Division* corresponds to one iGuard system, which may consist of a single iGuard unit or an iGuard Master/Slave configuration.

Only ONE iGuard can be registered with a particular Division, and this iGuard unit must be configured as a Master unit.

Each Division has an unique code called *Registration Code*. You need this code to register an iGuard to this Division.

You can find this code in the *Division Details* panel on this page.

You can find the instruction to register an iGuard unit to iGuardPayroll **here**.

SuperMaster (1 to n)

Division List

	Division	Mode	Reg. Code	IP Address	iGuard SN / Count
1	Exhibition	1 to 1	A63713	192.168.1.194:80 offline	VK-2003-528F-DAAF
2	iGuardExpress Demo	iGuardExpress	---	n/a	Count: 50
3	iGuardSystem Demo	1 to 1	691170	192.168.0.124:80 offline	VK-2003-521A-C252
4	iGuardSystem Demo-2	1 to 1	5B657A	192.168.1.181:80 offline	VK-2003-52A1-DAC1
5	mun101	1 to 1	B2235B	---	---
6	mun102	1 to 1	459118	---	---
7	SECON - iGuard Demo	1 to 1	759A61	192.168.1.3:80 offline	VK-2003-5227-C160
8	SuperMaster	SuperMaster (1 to n)	9AAA90	n/a	Count: 0

Details:

Division Details	
Name	Exhibition
Registration Code	A63713
iGuard SN	VK-2003-528F-DAAF
ID	RnB
Description	iGuard Security System
Firmware Version	5.0.9324
IP Address	192.168.1.194
Port	80
Created On	Sep 04, 2017 - 4:26 AM
iGuard Registered On	Sep 04, 2017 - 4:27 AM
Max. Employee Count	1000
Real Time Monitor	No

Delete Division | UnRegister iGuard | Edit

Tools

Connection Test:

Test Status: Offline

Upload User Data to iGuard:

Upload

Slave Mode: In Slave Mode, you must specify the Master unit by entering the unit's IP address and Port number.

Alternatively, you can also connect a slave unit to iGuardPayroll cloud service. Unlike a Master unit, you can only assign a slave unit to a special "SuperMaster" iGuardPayroll account[10], and have this special account act as the Master unit of the slave iGuard.

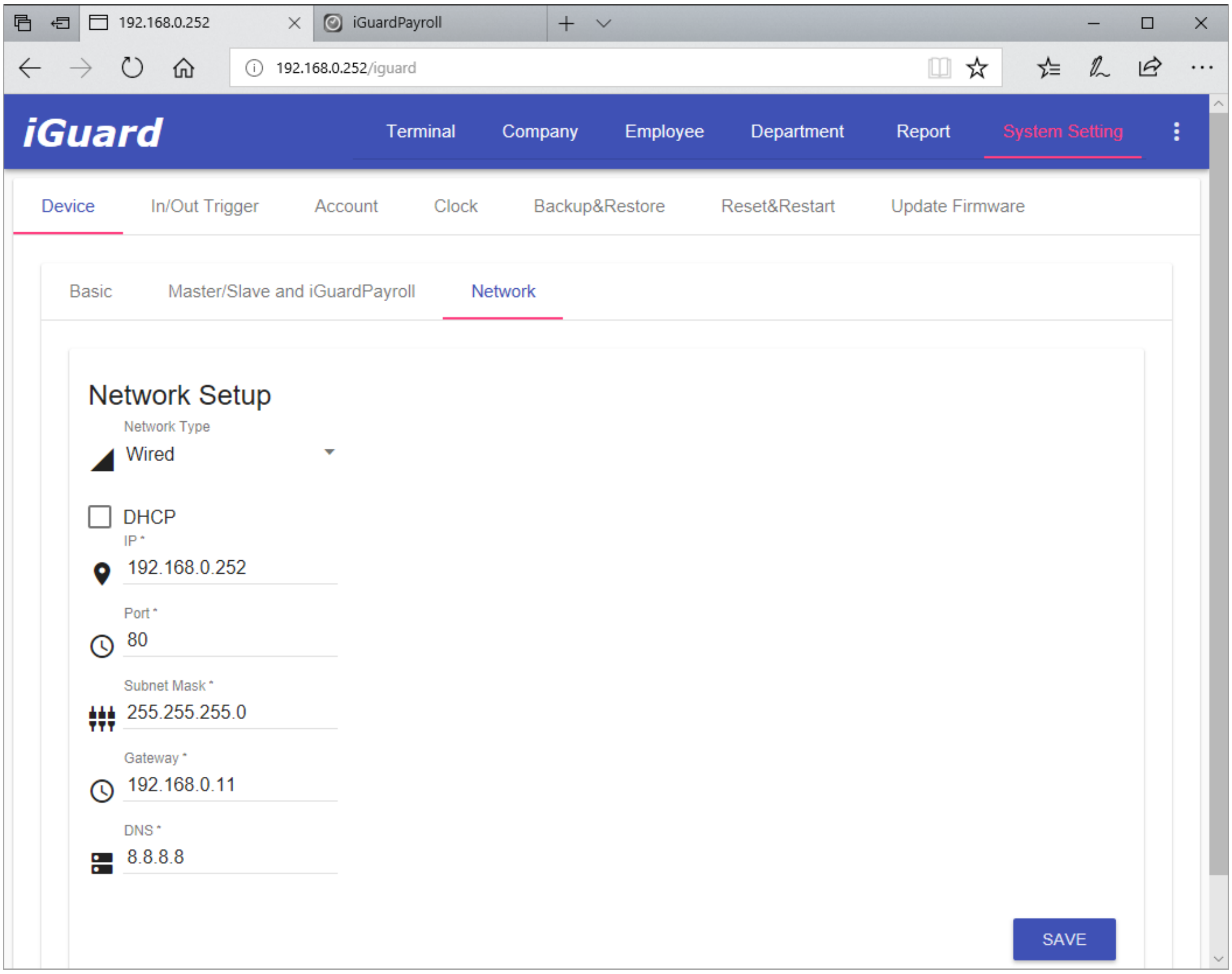
Network Setup

Use this page to configure the network setup of the unit.

It is suggested the network setting is assigned manually rather than using DHCP. This is especially true for Master unit, since all the slave units use the Master's IP address to locate the Master unit, and the DHCP server might change the Master's address every once in a while, causing connection lost problem.

A sample screen shot is as follow:

[10] iGuardPayroll's SuperMaster account is a paid service. Please contact your local reseller or visit www.iguardpayroll.com for more information.



Network Setup

Network Type: Wired

□ DHCP

IP *: 192.168.0.252

Port *: 80

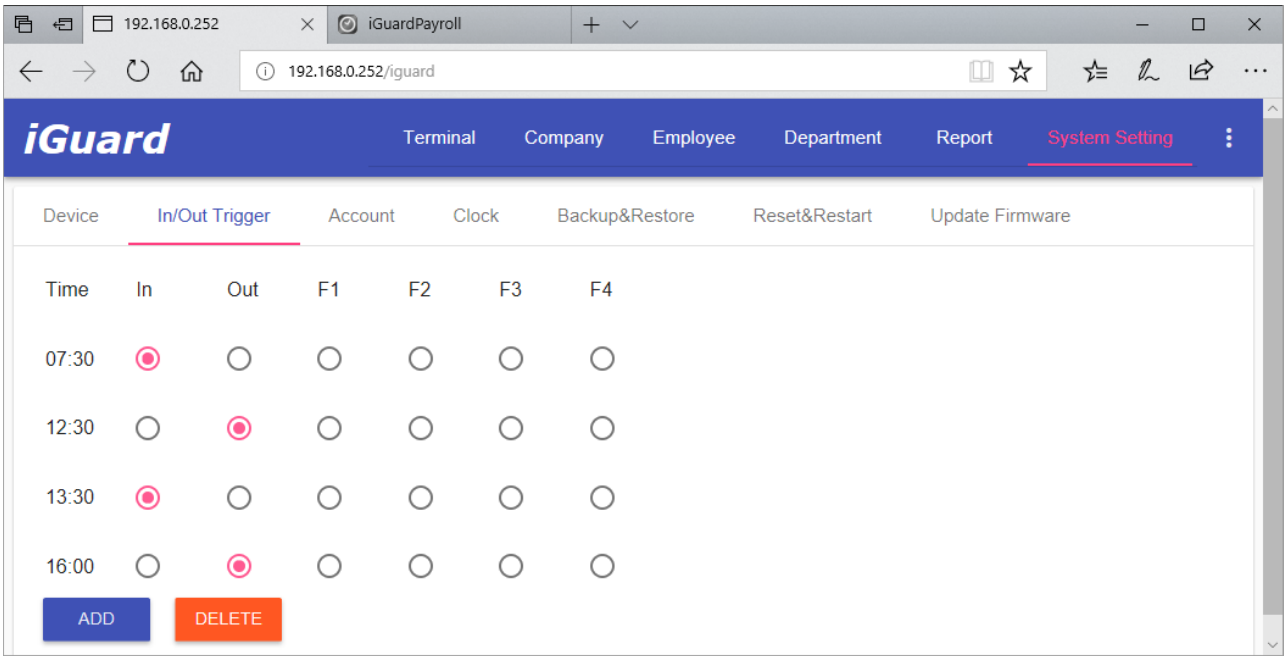
Subnet Mask *: 255.255.255.0

Gateway *: 192.168.0.11

DNS *: 8.8.8.8

In/Out Trigger

Use this page to set triggers for the IN / OUT setting. At the specified time, the default access status will automatically set to IN, and the unit clocks-in anyone who accesses the unit. The same applies for other access statuses like OUT, F1, F2 … etc.



Time	In	Out	F1	F2	F3	F4
07:30	●	○	○	○	○	○
12:30	○	●	○	○	○	○
13:30	●	○	○	○	○	○
16:00	○	●	○	○	○	○

In this example screenshot above, when the time reaches 7:30 in the morning, the default access status will change from OUT to IN. Likewise, the device will change the default status to OUT at 12:30, to IN at 13:30, and to OUT at 16:00, as shown in the following:-

Description	***LCD Display***
1. The default access status is OUT at 7:29	**Thu Aug 30 07:29** **ID #:_ OUT**
2. The default access status changes to IN at 7:30, to OUT at 12:30, to IN again at 13:30, and back to OUT at 16:00.	**Thu Aug 30 07:00** **ID #:_ IN** **:** **Thu Aug 30 12:30** **ID #:_ OUT** **:** **Thu Aug 30 13:30** **ID #:_ IN** **:** **Thu Aug 30 16:00** **ID #:_ OUT**

Note: The user can always override this default access status by pressing the *Backspace* key a few times until the desired access status is displayed on the LCD before entering the ID.

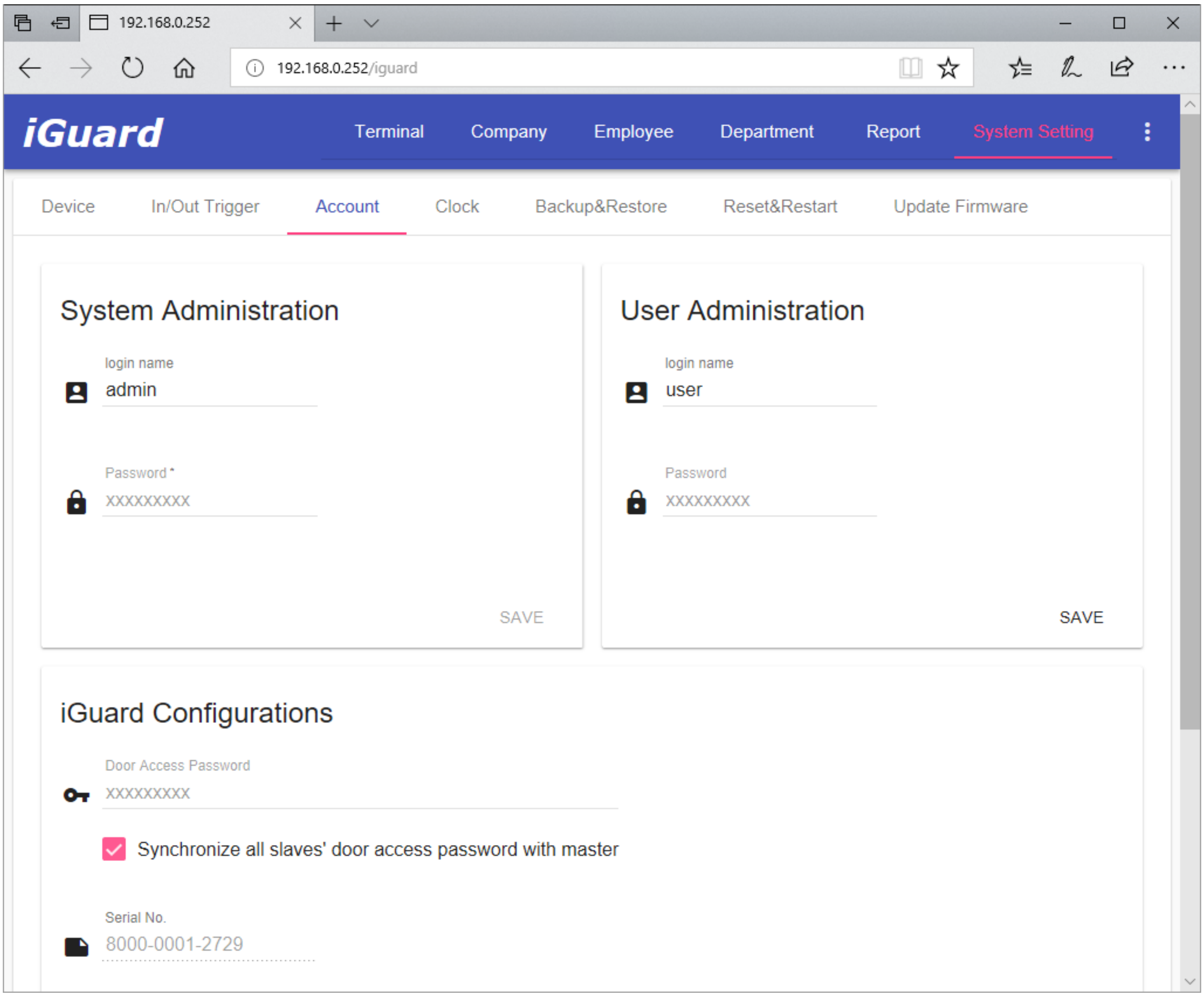
The entry can be removed by simply clicking on the **DELETE** button, then select the entries you would like delete, then press the **FINISHED** button.

Account

Use this page to set up the System Administrator’s login name and password, and User Administrator’s login name and password.

The Door Access Password can also be set here.

The following is a sample screen shot:



System Administration

login name: admin

Password *: XXXXXXXXX

User Administration

login name: user

Password: XXXXXXXXX

iGuard Configurations

Door Access Password: XXXXXXXXX

☑ Synchronize all slaves' door access password with master

Serial No.: 8000-0001-2729

The first entry is the System Administrator’s User Name & Password, which are required when accessing and modifying user information and system configuration. The valid characters for the password are 0-9, A & B, i.e., the characters one can enter using the iGuard keypad.

A Note on Master/Slave Configuration: The System Administrator Password of the Slave unit must be the same as the Master unit. Otherwise, the Master unit will reject the slave unit. In this case, an error message will be shown on the LCD display of the slave unit.

The second entry is the User Administrator’s User Name & Password. This is for accessing and modifying the user information (e.g. to add and delete users, and to assign & modify departments). However, it cannot be used to access and modify any system-related configuration (e.g. to change the IP address of the unit).

The last entry is the Door Access Password, which is used for the Quick Access purpose (please refer to the *Quick Access* section[11] earlier in this chapter in how to set up the Quick Access period).

[11] On page *Company* → *Setup* → *Quick Access Setup* (p. 40)

The following steps illustrate how to use the *Quick Access Password* to gain access:-

Description ***LCD Display***

1. While in Standby Mode, press the **Func** key. The unit will prompt you for the password.

```
Enter Password:
_
```

2. Enter the *Quick Access Password.*

```
Enter Password:
******_
```

3. Press **Func** key to confirm. If it is within the Quick Access Period, and this particular iGuard has been enabled for the Quick Access, the user will be authorized. The unit will return to Standby Mode.

```

Authorized!
```

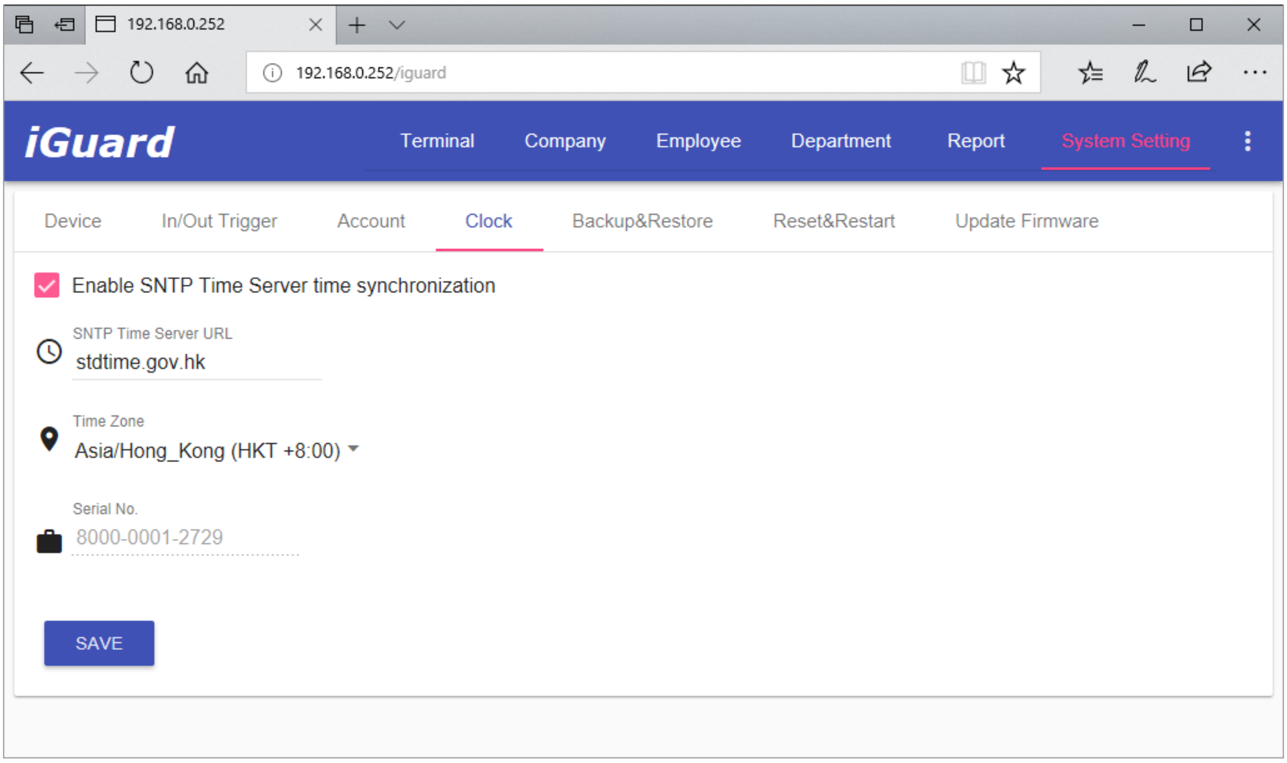
:

```
Thu Aug 30 15:02
ID #:_        IN
```

Unlike the other two administrator passwords, the Door Access Password can be configured as system-wise or unit-wise, by checking or clearing the checkbox of the "*Synchronize door access password with master*" option on the webpage. If it is configured as unit-wise, each slave can independently have its own Door Access Password.

Clock

Use this page to setup the SNTP Time Server URL and the Time Zone.



☑ Enable SNTP Time Server time synchronization

SNTP Time Server URL: stdtime.gov.hk

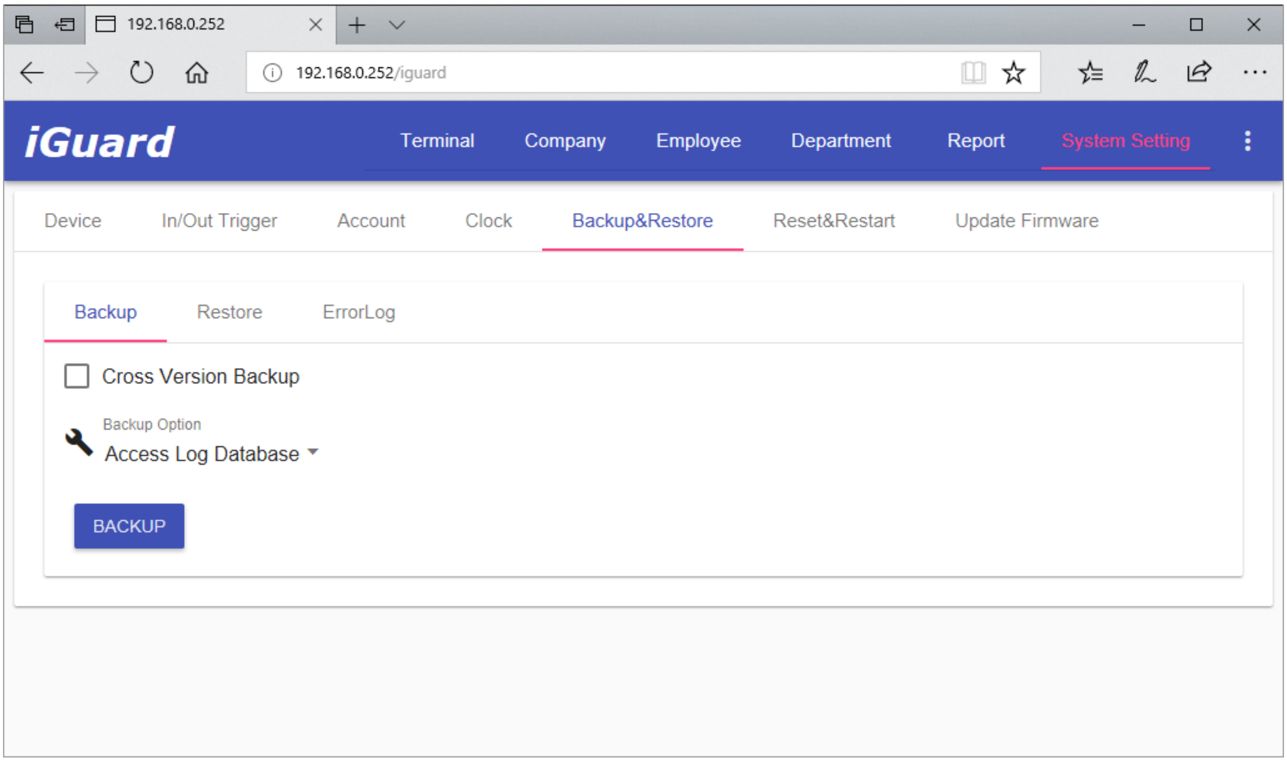
Time Zone: Asia/Hong_Kong (HKT +8:00)

Serial No.: 8000-0001-2729

Backup & Restore

We suggest backing up the internal user data & access log regularly to the desktop computer. In the unlikely event that the system is to be replaced or the database file is corrupted, the old data can be restored back to the device, and the employees do not need to re-register.

The following is the Backup & Restore page:



□ Cross Version Backup

Backup Option
Access Log Database

<u>Backup</u> – You can choose to back either the Employee Database or the Access Log. The default filename of the backup file is yyyymmddhhmmss.idb (e.g., 20180423120317.idb). This backup file can be restored to any LM530 machines. However, if you need to restore the data to legacy machines (such as LM520 models), check the "*Cross Version Backup*" option.

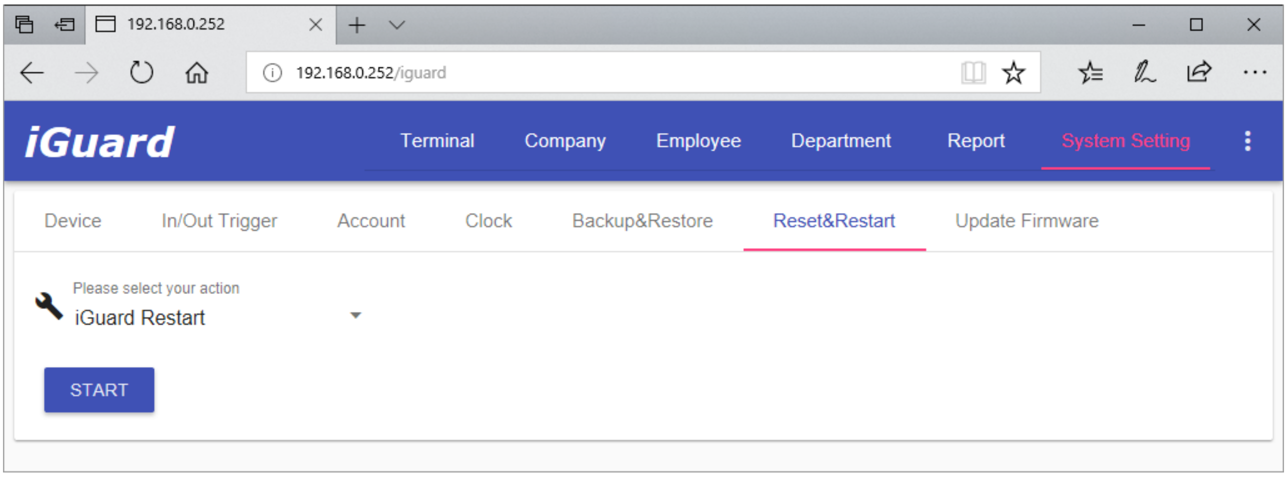
<u>Restore</u> – Use this page to restore the data from the backup file when it is necessary (for example, a new device has been installed).

You need to specify if you are to restore the employee data or the access log records. Ii is because in the legacy iGuard version, the backup file can contain both the employee data and the access log records.

iGuard can automatically detect the type of backup file, and will restore the data accordingly.

Reset & Restart

Use this page to remotely reset or shutdown the iGuard machine.



Please select your action: iGuard Restart

There are four options:

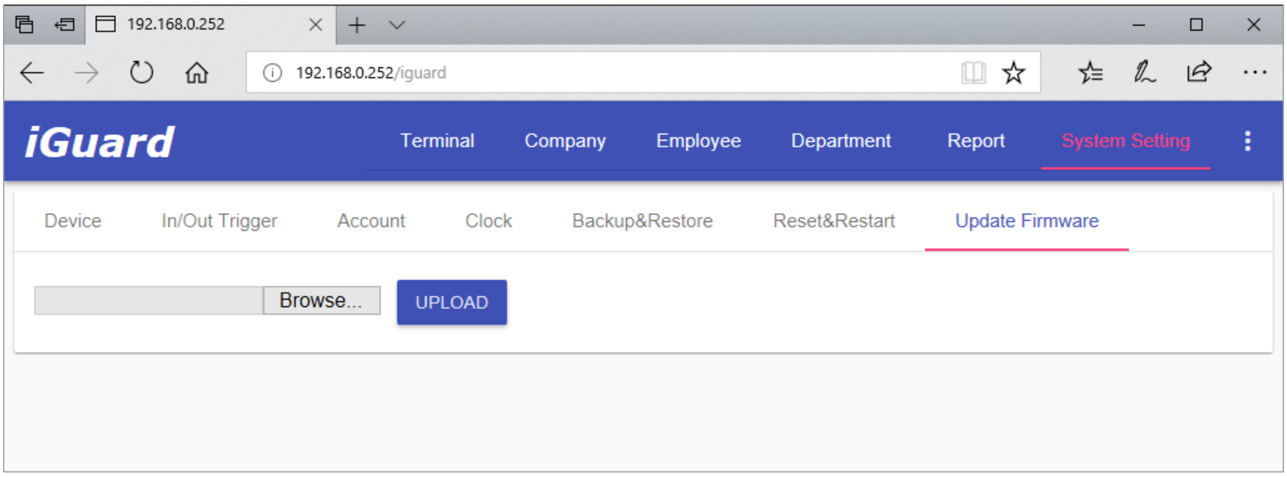
iGuard Restart – select this one to restart the device.

Purge Access Log – select this option to delete all the access logs. After the device has restarted, the access log will become empty.

Purge User Data – select this option to remove all employees information.

Factory Reset – this is for resetting all the device settings to factory default, and to reset the user & access log database. This is analogous to the *Function 7: Shutdown / Reset* in the keypad function menu discussed earlier.

Update Firmware



Should update the firmware of the device be necessary, you will receive a patch file containing the latest firmware. Use this page then to update the firmware of the device.

APPENDIX

Fingerprint Enrollment (for model LM530-FOSC only)

Fingerprint Enrollment is the process of registering the fingerprint template for later recognition.

A good enrollment is crucial for all fingerprint recognition systems in the market, including iGuard. A good fingerprint image captured during the enrollment process will significantly reduce the false-reject rate during later verification.

iGuard takes advantage of the latest optical sensor technology. However, as individuals, our hands may have different levels of moisture. In some cases, iGuard may have difficulty in recognizing some users' fingerprint images (mostly the people with dry skin problems). The problem is more noticeable during the enrollment process since the device requires a more accurate and higher quality fingerprint image than the normal verification process.

The easiest way to get around the dry skin problem is to apply a small amount of moisturizing lotion on the dry skin during the enrollment process. *This step is only required in the enrollment stage, and will not be needed in the daily routine verification process.*

For users with wet skin problems, simply wipe the finger with cloth or paper towel before having any contact with the fingerprint sensor. Please note that excessive sweat *will* reduce the normal life time of the fingerprint sensor.

The image quality can be improved tremendously by taking care of the dry and wet skin condition discussed above. It is important that the user stores a high quality image during enrollment, because this is the fingerprint image that the device will use to compare against the submitted fingerprint images in all the verifications later on. If the users’ enrolled fingerprint image is of low quality, the user may get unexpected results during the verification stage later on.

Here are some other general factors that may influence the enrollment:

- **Finger Position**. Always align the center of the fingerprint with the center of the fingerprint sensor. Do not use the tip of the finger, and do not place the finger too much to the left or to the right. Otherwise, false reject may occur.

- **Finger area**. It is best to cover the sensor area completely with the fingerprint to ensure the maximum fingerprint surface contact area. A common mistake is to touch the sensor with the tip of the finger, which contains too few minutiae points. It is also best to use the thumbs rather than other fingers.

- **Finger rotation**. Keep fingerprint rotation minimal during the enrollment

- **Finger pressure**. Use medium pressure. Excessive pressure may distort the image and may adhere ridges together

iGuardPayroll

iGuardPayroll is a free, cloud-based service for all iGuard users. It works seamlessly with all iGuard models, providing essential payroll functions for your company. Unlike other payroll applications in the market, iGuardPayroll is free to use for all iGuard users.

With this service, all the iGuard data, such as employees' access log records, is automatically transmitted from iGuardExpress & iGuard machines to iGuardPayroll in real-time manner. Its cloud-based storage can store up to 1,000,000 (or up to five years) records, providing maintenance-free and reliable storage for your company.

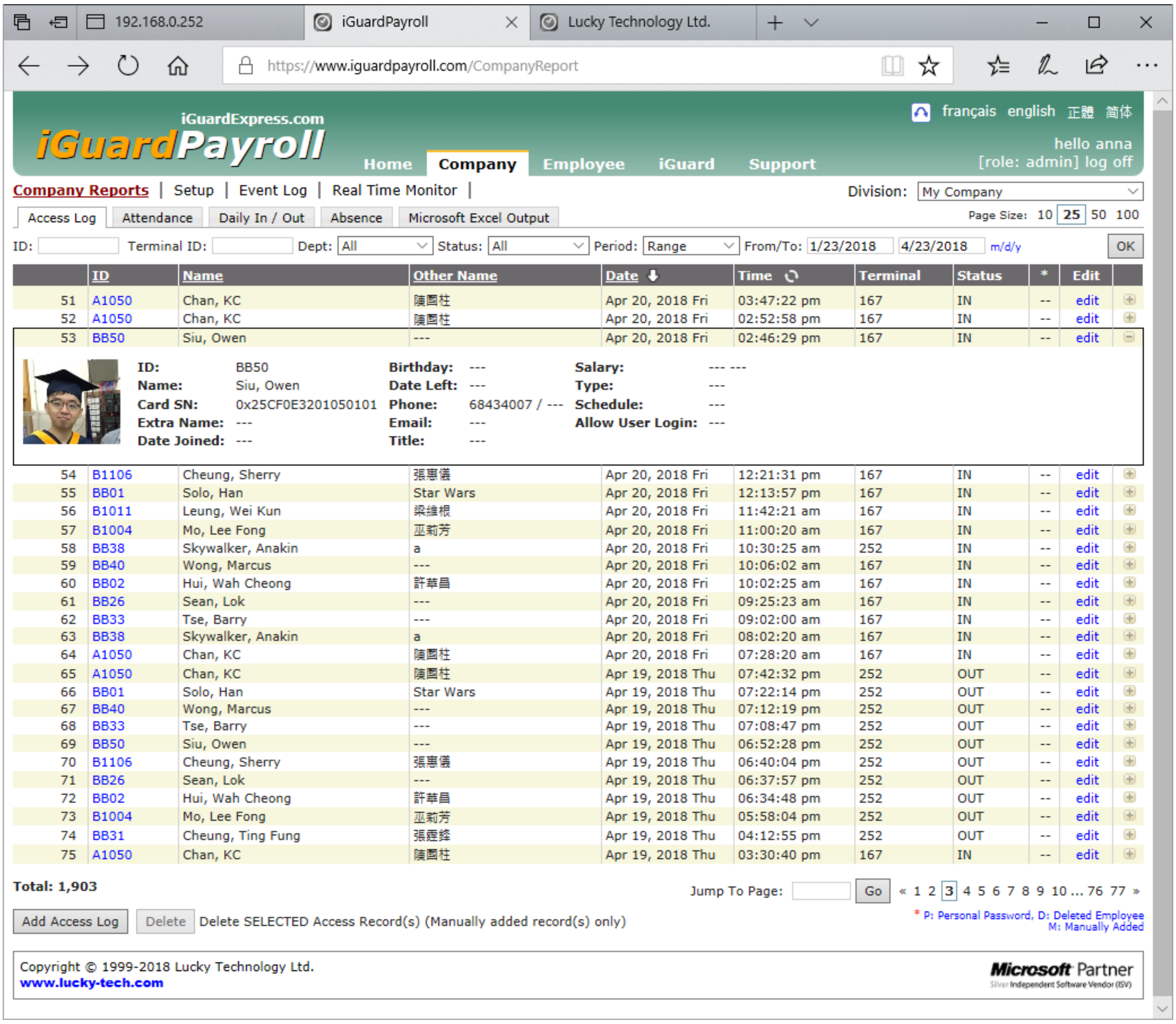
It helps you manage your employees' information and provides a lot of management reports, such as late reports, leave reports and more.

Please visit www.iguardpayroll.com for more information.

The following are some of the features with screen shots.

1. Access Log with Employee Details

iGuardPayroll can store up to 1,000,000 (or up to five years) records for free.



Division: My Company

Page Size: 10 25 50 100

ID: Terminal ID: Dept: All Status: All Period: Range From/To: 1/23/2018 4/23/2018 m/d/y

	ID	Name	Other Name	Date	Time	Terminal	Status	*	Edit	
51	A1050	Chan, KC	陳國柱	Apr 20, 2018 Fri	03:47:22 pm	167	IN	--	edit	⊞
52	A1050	Chan, KC	陳國柱	Apr 20, 2018 Fri	02:52:58 pm	167	IN	--	edit	⊞
53	BB50	Siu, Owen	---	Apr 20, 2018 Fri	02:46:29 pm	167	IN	--	edit	⊟

ID:	BB50	**Birthday:**	---	**Salary:**	--- ---
Name:	Siu, Owen	**Date Left:**	---	**Type:**	---
Card SN:	0x25CF0E3201050101	**Phone:**	68434007 / ---	**Schedule:**	---
Extra Name:	---	**Email:**	---	**Allow User Login:**	---
Date Joined:	---	**Title:**	---		

	ID	Name	Other Name	Date	Time	Terminal	Status	*	Edit	
54	B1106	Cheung, Sherry	張惠儀	Apr 20, 2018 Fri	12:21:31 pm	167	IN	--	edit	⊞
55	BB01	Solo, Han	Star Wars	Apr 20, 2018 Fri	12:13:57 pm	167	IN	--	edit	⊞
56	B1011	Leung, Wei Kun	梁維根	Apr 20, 2018 Fri	11:42:21 am	167	IN	--	edit	⊞
57	B1004	Mo, Lee Fong	巫莉芳	Apr 20, 2018 Fri	11:00:20 am	167	IN	--	edit	⊞
58	BB38	Skywalker, Anakin	a	Apr 20, 2018 Fri	10:30:25 am	252	IN	--	edit	⊞
59	BB40	Wong, Marcus	---	Apr 20, 2018 Fri	10:06:02 am	167	IN	--	edit	⊞
60	BB02	Hui, Wah Cheong	許華昌	Apr 20, 2018 Fri	10:02:25 am	167	IN	--	edit	⊞
61	BB26	Sean, Lok	---	Apr 20, 2018 Fri	09:25:23 am	167	IN	--	edit	⊞
62	BB33	Tse, Barry	---	Apr 20, 2018 Fri	09:02:00 am	167	IN	--	edit	⊞
63	BB38	Skywalker, Anakin	a	Apr 20, 2018 Fri	08:02:20 am	167	IN	--	edit	⊞
64	A1050	Chan, KC	陳國柱	Apr 20, 2018 Fri	07:28:20 am	167	IN	--	edit	⊞
65	A1050	Chan, KC	陳國柱	Apr 19, 2018 Thu	07:42:32 pm	252	OUT	--	edit	⊞
66	BB01	Solo, Han	Star Wars	Apr 19, 2018 Thu	07:22:14 pm	252	OUT	--	edit	⊞
67	BB40	Wong, Marcus	---	Apr 19, 2018 Thu	07:12:19 pm	252	OUT	--	edit	⊞
68	BB33	Tse, Barry	---	Apr 19, 2018 Thu	07:08:47 pm	252	OUT	--	edit	⊞
69	BB50	Siu, Owen	---	Apr 19, 2018 Thu	06:52:28 pm	252	OUT	--	edit	⊞
70	B1106	Cheung, Sherry	張惠儀	Apr 19, 2018 Thu	06:40:04 pm	252	OUT	--	edit	⊞
71	BB26	Sean, Lok	---	Apr 19, 2018 Thu	06:37:57 pm	252	OUT	--	edit	⊞
72	BB02	Hui, Wah Cheong	許華昌	Apr 19, 2018 Thu	06:34:48 pm	252	OUT	--	edit	⊞
73	B1004	Mo, Lee Fong	巫莉芳	Apr 19, 2018 Thu	05:58:04 pm	252	OUT	--	edit	⊞
74	BB31	Cheung, Ting Fung	張霆鋒	Apr 19, 2018 Thu	04:12:55 pm	252	OUT	--	edit	⊞
75	A1050	Chan, KC	陳國柱	Apr 19, 2018 Thu	03:30:40 pm	167	IN	--	edit	⊞

Total: 1,903

Jump To Page: « 1 2 3 4 5 6 7 8 9 10 ... 76 77 »

Delete SELECTED Access Record(s) (Manually added record(s) only)

* P: Personal Password, D: Deleted Employee
M: Manually Added

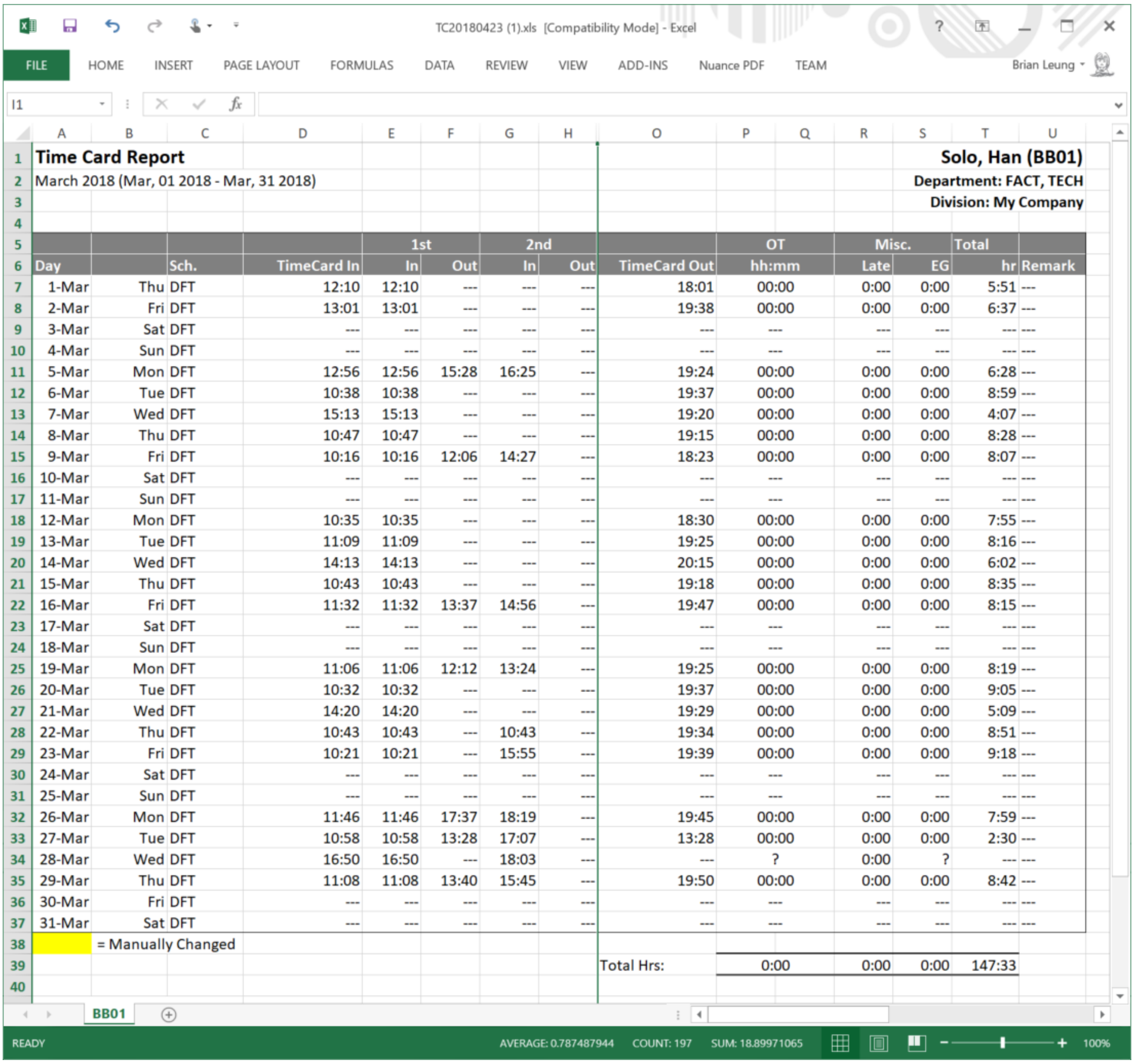
Copyright © 1999-2018 Lucky Technology Ltd.
www.lucky-tech.com

Microsoft Partner
Silver Independent Software Vendor (ISV)

2. Time Card Report in Excel Format output

In addition to displaying the reports in Internet Browser, most reports are available in Microsoft Excel format readily for download.

These reports are in real Excel format (i.e., not in csv format), therefore, it will be very easy to incorporate the information into any existing applications if necessary.



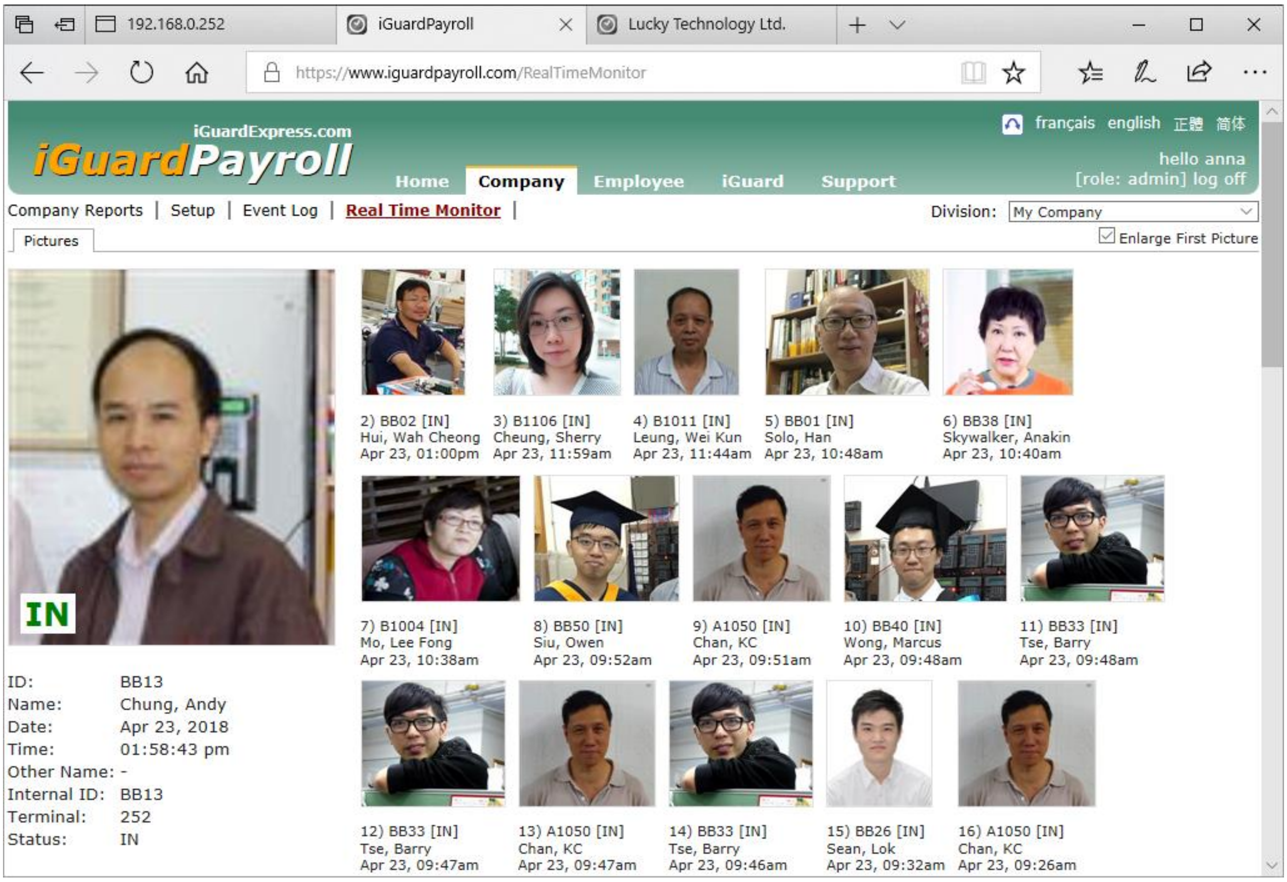
Time Card Report
March 2018 (Mar, 01 2018 - Mar, 31 2018)

Solo, Han (BB01)
Department: FACT, TECH
Division: My Company

				1st		2nd			OT	Misc.		Total	
Day		Sch.	TimeCard In	In	Out	In	Out	TimeCard Out	hh:mm	Late	EG	hr	Remark
1-Mar	Thu	DFT	12:10	12:10	---	---	---	18:01	00:00	0:00	0:00	5:51	---
2-Mar	Fri	DFT	13:01	13:01	---	---	---	19:38	00:00	0:00	0:00	6:37	---
3-Mar	Sat	DFT	---	---	---	---	---	---	---	---	---	---	---
4-Mar	Sun	DFT	---	---	---	---	---	---	---	---	---	---	---
5-Mar	Mon	DFT	12:56	12:56	15:28	16:25	---	19:24	00:00	0:00	0:00	6:28	---
6-Mar	Tue	DFT	10:38	10:38	---	---	---	19:37	00:00	0:00	0:00	8:59	---
7-Mar	Wed	DFT	15:13	15:13	---	---	---	19:20	00:00	0:00	0:00	4:07	---
8-Mar	Thu	DFT	10:47	10:47	---	---	---	19:15	00:00	0:00	0:00	8:28	---
9-Mar	Fri	DFT	10:16	10:16	12:06	14:27	---	18:23	00:00	0:00	0:00	8:07	---
10-Mar	Sat	DFT	---	---	---	---	---	---	---	---	---	---	---
11-Mar	Sun	DFT	---	---	---	---	---	---	---	---	---	---	---
12-Mar	Mon	DFT	10:35	10:35	---	---	---	18:30	00:00	0:00	0:00	7:55	---
13-Mar	Tue	DFT	11:09	11:09	---	---	---	19:25	00:00	0:00	0:00	8:16	---
14-Mar	Wed	DFT	14:13	14:13	---	---	---	20:15	00:00	0:00	0:00	6:02	---
15-Mar	Thu	DFT	10:43	10:43	---	---	---	19:18	00:00	0:00	0:00	8:35	---
16-Mar	Fri	DFT	11:32	11:32	13:37	14:56	---	19:47	00:00	0:00	0:00	8:15	---
17-Mar	Sat	DFT	---	---	---	---	---	---	---	---	---	---	---
18-Mar	Sun	DFT	---	---	---	---	---	---	---	---	---	---	---
19-Mar	Mon	DFT	11:06	11:06	12:12	13:24	---	19:25	00:00	0:00	0:00	8:19	---
20-Mar	Tue	DFT	10:32	10:32	---	---	---	19:37	00:00	0:00	0:00	9:05	---
21-Mar	Wed	DFT	14:20	14:20	---	---	---	19:29	00:00	0:00	0:00	5:09	---
22-Mar	Thu	DFT	10:43	10:43	---	10:43	---	19:34	00:00	0:00	0:00	8:51	---
23-Mar	Fri	DFT	10:21	10:21	---	15:55	---	19:39	00:00	0:00	0:00	9:18	---
24-Mar	Sat	DFT	---	---	---	---	---	---	---	---	---	---	---
25-Mar	Sun	DFT	---	---	---	---	---	---	---	---	---	---	---
26-Mar	Mon	DFT	11:46	11:46	17:37	18:19	---	19:45	00:00	0:00	0:00	7:59	---
27-Mar	Tue	DFT	10:58	10:58	13:28	17:07	---	13:28	00:00	0:00	0:00	2:30	---
28-Mar	Wed	DFT	16:50	16:50	---	18:03	---	---	?	0:00	?	---	---
29-Mar	Thu	DFT	11:08	11:08	13:40	15:45	---	19:50	00:00	0:00	0:00	8:42	---
30-Mar	Fri	DFT	---	---	---	---	---	---	---	---	---	---	---
31-Mar	Sat	DFT	---	---	---	---	---	---	---	---	---	---	---
🟨	= Manually Changed												
								Total Hrs:	0:00	0:00	0:00	147:33	

3. Real Time Monitor

An optional feature of iGuardPayroll is to show the pictures of the employees who had just clocked-in & clocked-out. It provides a very handy tool for the management, for example, to monitor the employees and to know immediately who had just arrived or left the company.



Company Reports | Setup | Event Log | **Real Time Monitor** |

Division: My Company

Pictures

☑ Enlarge First Picture

ID:	BB13
Name:	Chung, Andy
Date:	Apr 23, 2018
Time:	01:58:43 pm
Other Name:	-
Internal ID:	BB13
Terminal:	252
Status:	IN

2) BB02 [IN]
Hui, Wah Cheong
Apr 23, 01:00pm

3) B1106 [IN]
Cheung, Sherry
Apr 23, 11:59am

4) B1011 [IN]
Leung, Wei Kun
Apr 23, 11:44am

5) BB01 [IN]
Solo, Han
Apr 23, 10:48am

6) BB38 [IN]
Skywalker, Anakin
Apr 23, 10:40am

7) B1004 [IN]
Mo, Lee Fong
Apr 23, 10:38am

8) BB50 [IN]
Siu, Owen
Apr 23, 09:52am

9) A1050 [IN]
Chan, KC
Apr 23, 09:51am

10) BB40 [IN]
Wong, Marcus
Apr 23, 09:48am

11) BB33 [IN]
Tse, Barry
Apr 23, 09:48am

12) BB33 [IN]
Tse, Barry
Apr 23, 09:47am

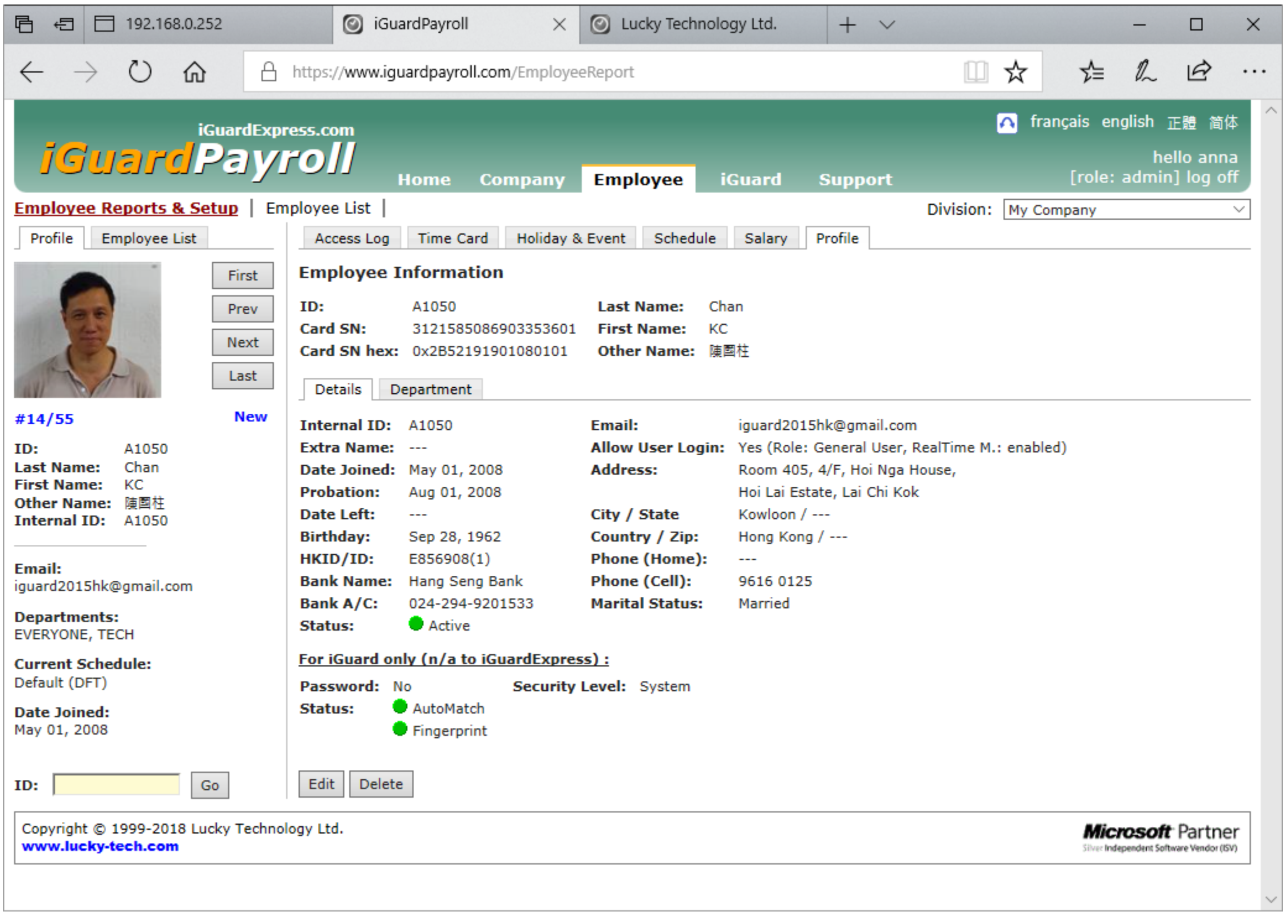
13) A1050 [IN]
Chan, KC
Apr 23, 09:47am

14) BB33 [IN]
Tse, Barry
Apr 23, 09:46am

15) BB26 [IN]
Sean, Lok
Apr 23, 09:32am

16) A1050 [IN]
Chan, KC
Apr 23, 09:26am

4. Employee Profile



Employee Reports & Setup | Employee List |

Division: My Company

Profile | Employee List

Access Log | Time Card | Holiday & Event | Schedule | Salary | Profile

#14/55 **New**

ID:	A1050
Last Name:	Chan
First Name:	KC
Other Name:	陳國柱
Internal ID:	A1050

Email:
iguard2015hk@gmail.com

Departments:
EVERYONE, TECH

Current Schedule:
Default (DFT)

Date Joined:
May 01, 2008

ID: Go

Employee Information

ID:	A1050	**Last Name:**	Chan
Card SN:	3121585086903353601	**First Name:**	KC
Card SN hex:	0x2B52191901080101	**Other Name:**	陳國柱

Details | Department

Internal ID:	A1050	**Email:**	iguard2015hk@gmail.com
Extra Name:	---	**Allow User Login:**	Yes (Role: General User, RealTime M.: enabled)
Date Joined:	May 01, 2008	**Address:**	Room 405, 4/F, Hoi Nga House,
Probation:	Aug 01, 2008		Hoi Lai Estate, Lai Chi Kok
Date Left:	---	**City / State**	Kowloon / ---
Birthday:	Sep 28, 1962	**Country / Zip:**	Hong Kong / ---
HKID/ID:	E856908(1)	**Phone (Home):**	---
Bank Name:	Hang Seng Bank	**Phone (Cell):**	9616 0125
Bank A/C:	024-294-9201533	**Marital Status:**	Married
Status:	● Active		

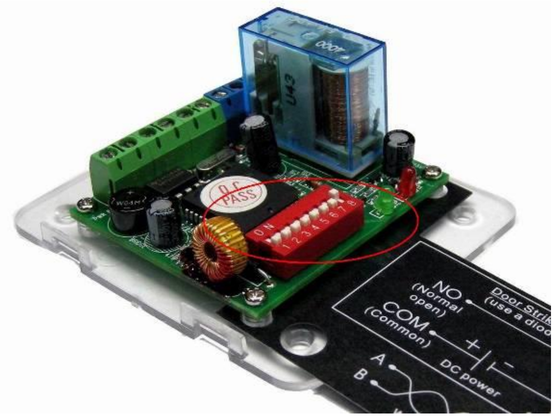
For iGuard only (n/a to iGuardExpress) :

Password:	No	**Security Level:**	System
Status:	● AutoMatch ● Fingerprint		

Copyright © 1999-2018 Lucky Technology Ltd.
www.lucky-tech.com

Remote Door Relay

The iGuard capabilities can be enhanced by the use of the Remote Door Relay, which is sold separately from the iGuard unit. The Remote Relay assures that malicious damage to or tampering with the iGuard does not result in a release of the electric door strike or magnetic lock.



This device is to be physically installed inside the premises, and it is connected to the iGuard’s *Remote Relay* connector at the back of the unit through a special twisted-pair cable.

When using the relay, the electric door strike actions are controlled by the remote door relay rather than directly by the iGuard unit. The remote relay will only release the strike / lock when a properly addressed Release-and-Relock signal is received from the iGuard unit to which it is attached.

The use of the relay is recommended for all access control installations, and is required when controlling a 12VDC electric door strike or magnetic lock with a current rating above 1Amp.

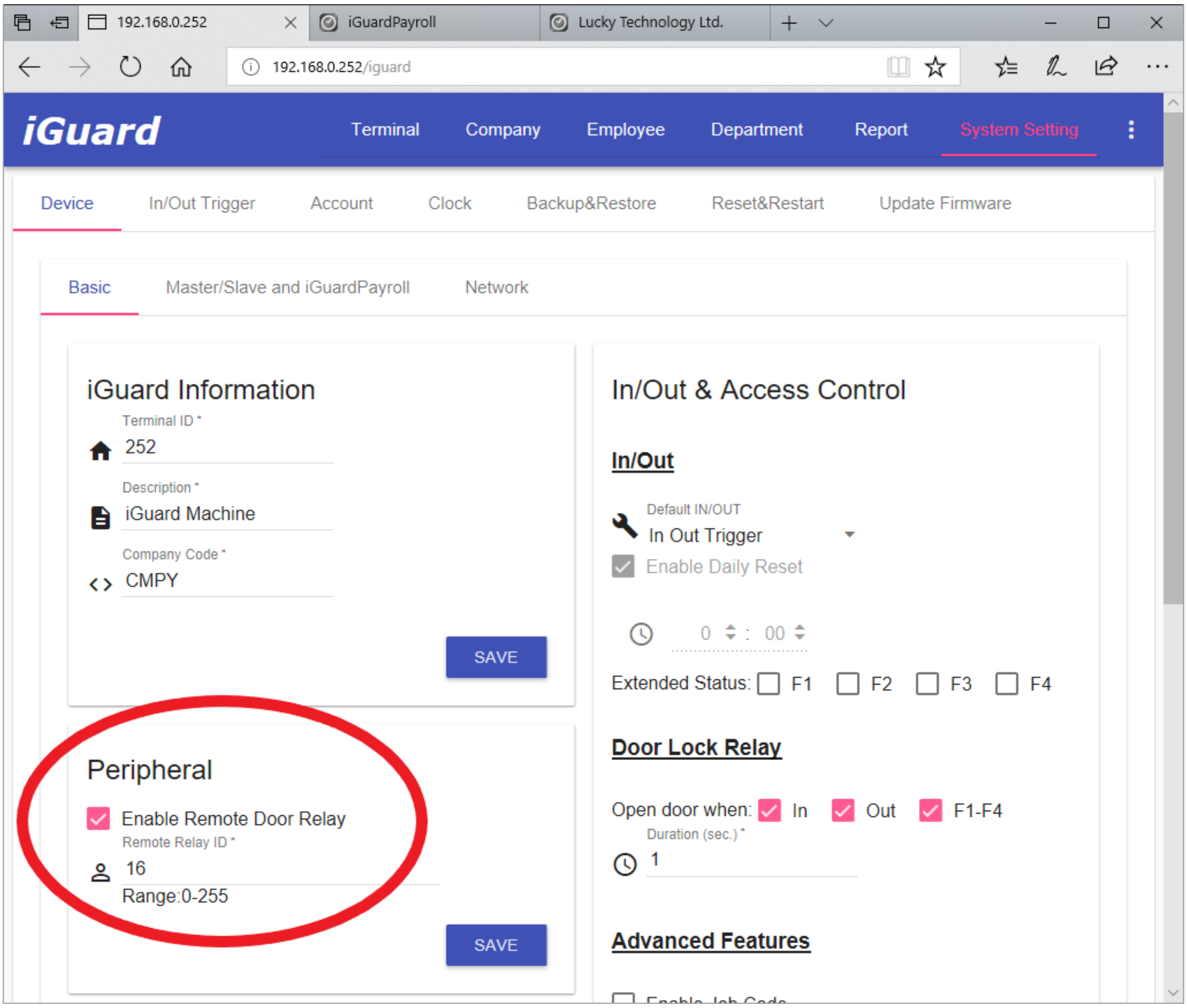
Configuration

Before installing the relay, set the Remote Relay ID with the 8-Bit Jumper switches on the relay (circled in red in the above picture). The chart below explains how to calculate the value that the switches are set to. Add the Numeric Value of each switch you turn to the ‘On’ position. This total will be the ID value of the Relay.

Switch Number	Numeric Value
1	1
2	2
3	4
4	8
5	16
6	32
7	64
8	128

For Example, if the switches 3 and 7 are turned to 'ON', the value is 68 (i.e., 4 + 64 = 68). If all switches are turned to 'ON', the value is 255.

The same ID must ***also*** be specified in the webpage as shown in the screen shot below, and the *Output Enable* checkbox must also be checked.



iGuard Information

Terminal ID * 252

Description * iGuard Machine

Company Code * CMPY

Peripheral

☑ Enable Remote Door Relay

Remote Relay ID * 16

Range:0-255

In/Out & Access Control

In/Out

Default IN/OUT: In Out Trigger

☑ Enable Daily Reset

0 : 00

Extended Status: □ F1 □ F2 □ F3 □ F4

Door Lock Relay

Open door when: ☑ In ☑ Out ☑ F1-F4

Duration (sec.) * 1

Advanced Features

□ Enable Job Code

The following is the connection terminals of the Remote Relay:

Terminal	Label	Description
1	NO	Door Relay's Normal Open
2	COM	Door Relay's Common
3	NC	Door Relay's Normal Close
4 & 5	DOOR SW	Door Switch
6	A – RS485	Connect to iGuard
7	B – RS485	Connect to iGuard
8	+12V DC	+12V DC
9	GND	Power Ground

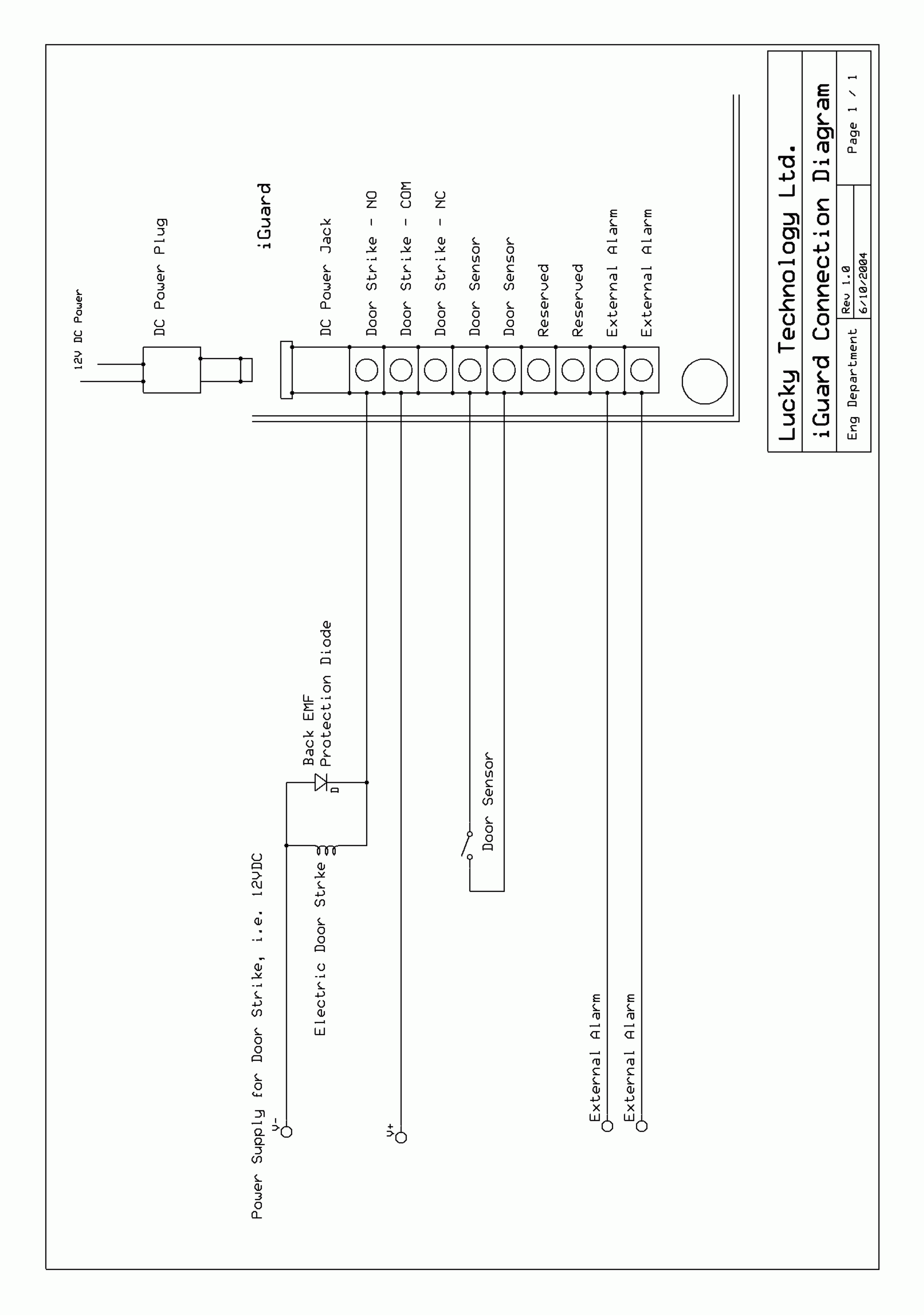
Care must be taken when connecting the two twisted-pair wire to the devices, and do not mix up the two labels, A & B, and the corresponding terminals of the Remote Relay device.

Warning: A twisted pair of wire must be used to connect the iGuard and the Remote Relay device. Otherwise, the wire may pick up the noise in the environment (such as the noise generated from the power wire nearby), and may make the device malfunction.

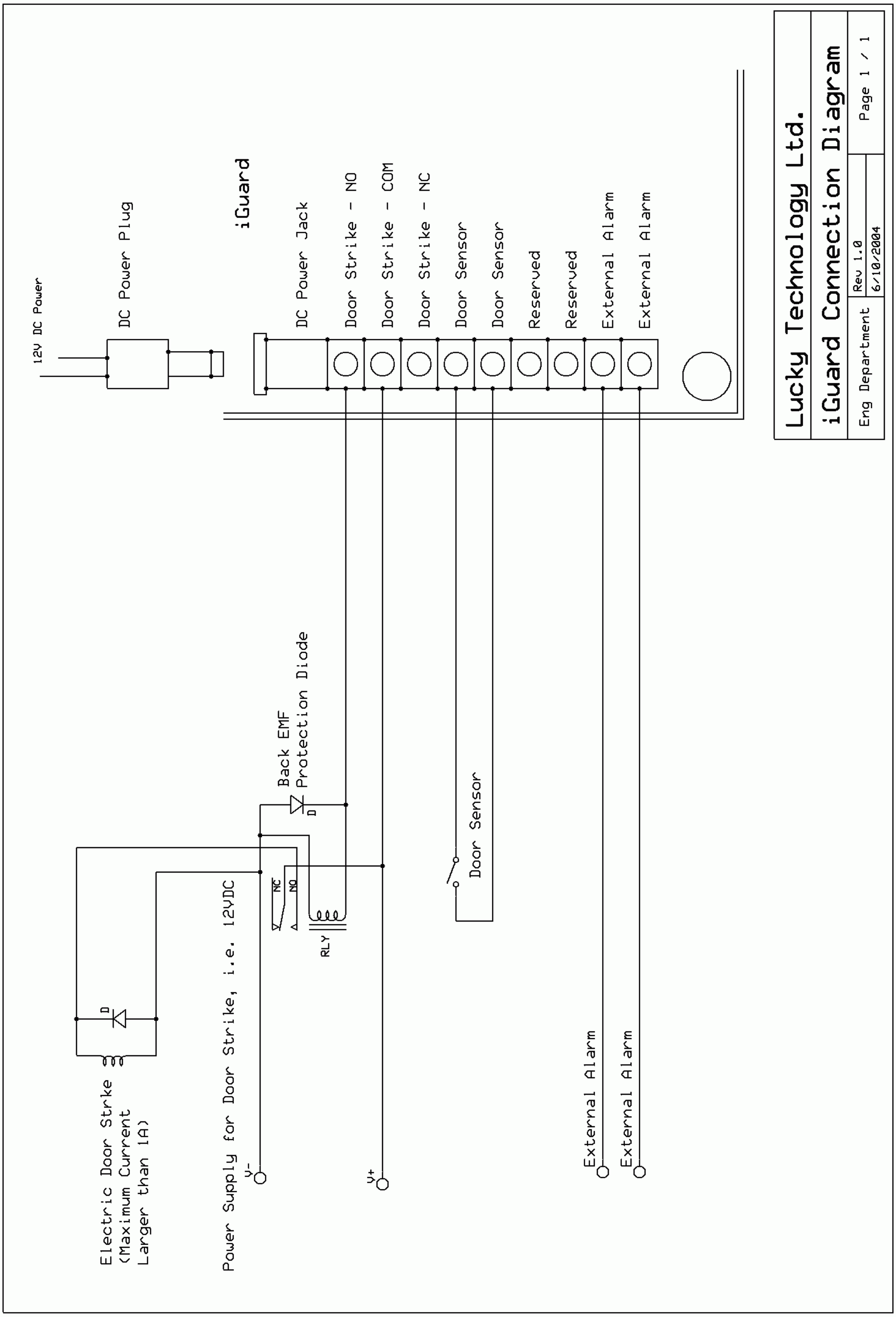
# # # # #

Connection Diagram

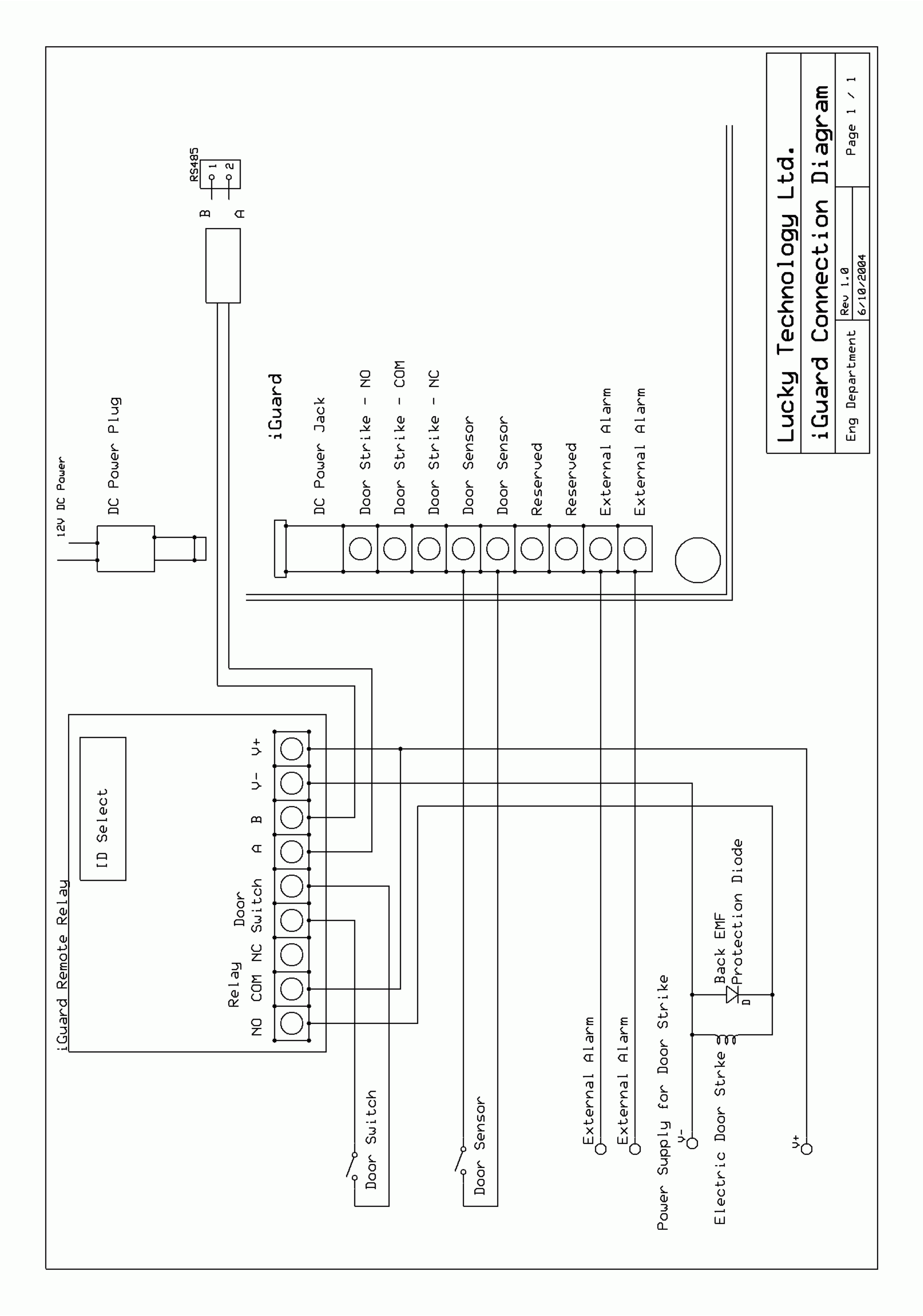
Basic Connection



Basic Connection (Large Load)



Remote Relay



Contact Information

Lucky Technology Ltd.

Address: 2/F, Flat A-D, Wah Hing Industrial Mansion, 36 Tai Yau Street
San Po Kong, Kowloon, Hong Kong
Telephone: 852-3176-6056
Fax: 852-3012-1980
Email: sales@lucky.com.hk

Website: www.lucky-tech.com

# # # # #

LUCKY

Technology Ltd.

Lucky Technology Ltd.

www.lucky-tech.com