iGuard™ LM Series

Operation Manual

Version 3.6.xxxx

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: FPS110 / LM

Table of Content

1.INSTALLATION

1.1. Quick Installation

Before installing your iGuard, it is important to check a few criteria for safe and easy installation. For this, please read the pre-installation notes as listed below for your reference as to steps you should take before implementing iGuard.

1.1.1. Pre-Installation Notes

- The iGuard terminal is designed for indoor installation. If you wish to install it outdoors, you must beware of not exposing it to water or harsh conditions.
- During installation you must be sure of grounding the iGuard back metal panel to Earth to prevent electrical impulses and shocks from affecting users or the iGuard terminals.
- To prevent electrical shortage or short-circuits, it is advised not to share the power supply of the iGuard with any other device, e.g. electrical lock.
- To ensure safety, do NOT connect the door button to the iGuard terminal. Instead connect it directly to the door strike, in case of power outage or other emergencies.
- To heighten the security level of the premises, do install the external relay together with the iGuard. This will increase security since the external relay is placed within office premises and not outdoors, as is the iGuard.
- Do NOT install the product next to heat emitting sources or in a place subject to direct sunlight or excessive dust.
- If smart card reader model is used, please make sure the Company Code is set. See Configuration.

1.1.2. Installation

Determine the location(s) for installing iGuard, external relay, door lock and power supply line. Fasten the rear metal panel at the location where the terminal will be installed. Connect the terminal with the power supply provided by the factory.

iGuard Terminal Connections

- Terminal #1 - Ground
- Terminal #2 - + 12V
- Terminal #3/4 - Normal Open
- Terminal #4/5 - Normal Close
- Terminal #6/7 - Door Sensor (optional)
- Terminal #8/9 – Reserved
- Terminal #10/11 - External Alarm (optional)
- Plug - External Relay Switch (optional)

iGuard can be connected directly to your corporate network via standard RJ-45 cable & TCP/IP protocols. Make sure your computer/notebook has been installed and configured with the TCP/IP Protocols.

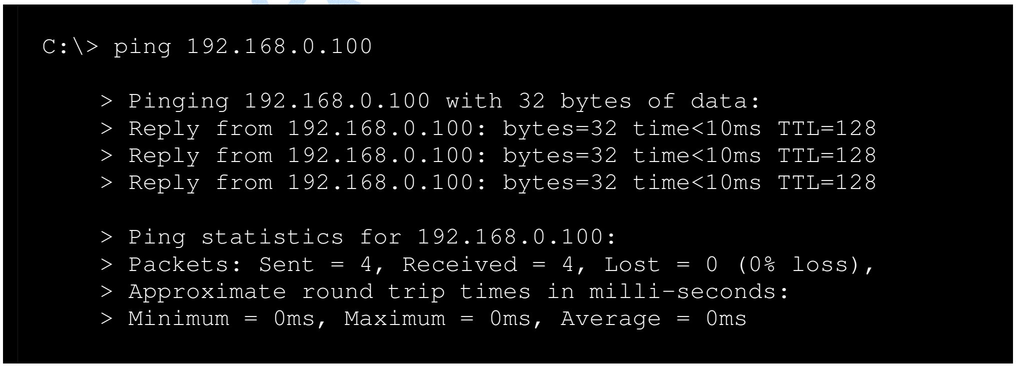
iGuard can also be connected directly to the network card of PC via crossover RJ-45 cable.

Setting Network and TCP/IP address

- On your iGuard, press **FUNC**, enter the default password "123", press **FUNC**, press **5**.
- Enter Date + **FUNC**.
- Enter Time + **FUNC**.
- Enter the device name + **FUNC** to continue.
- Enter IP address (depending on your corporate network addressing scheme, e.g. 192.168.0.101) + **FUNC** to continue.
- Enter Subnet Mask (depending on your corporate network addressing scheme, e.g. 255.255.255.0) + **FUNC** to continue.
- Enter Default Gateway + **FUNC** to continue.
- Enter DNS (optional) + **FUNC** to continue.
- Select Master/Slave Mode (1 for **Master** or 2 for **Slave**).
- Press **1** to accept these values or **2** to cancel.

To test whether the iGuard is functioning in the network, try to **PING** the device from your PC.

- On your PC, go to Run Command from Start Menu.
- Type 'ipconfig " to check the IP address of your PC and make sure it is in the same network as iGuard.
- Ping the IP address of iGuard, default: 192.168.0.100.
- If the ping responds the following, the IP is set properly and you are ready to proceed:



```
C:\> ping 192.168.0.100

    > Pinging 192.168.0.100 with 32 bytes of data:
    > Reply from 192.168.0.100: bytes=32 time<10ms TTL=128
    > Reply from 192.168.0.100: bytes=32 time<10ms TTL=128
    > Reply from 192.168.0.100: bytes=32 time<10ms TTL=128

    > Ping statistics for 192.168.0.100:
    > Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    > Approximate round trip times in milli-seconds:
    > Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Open your PC web browser, Internet Explorer or Netscape Navigator, and type in http://192.168.0.100 (IP Address of your iGuard), and you will be able to see iGuard's web interface in the browser window.

1.2. Power Requirements

iGuard requires a switching DC 12V / 500mA power supply. It is not recommended that the same power supply to be shared by both iGuard and the door strike because of the potential back E.M.F. Problem.

**Warning: Please do NOT use other power supplies since this may lead to system failure, and poor or unreliable operation.

1.3. Deciding where to install

iGuard is a wall-mounted unit with a miniscule footprint, and can be conveniently installed anywhere. However, 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, usually 5 seconds by default. Also note the following points:

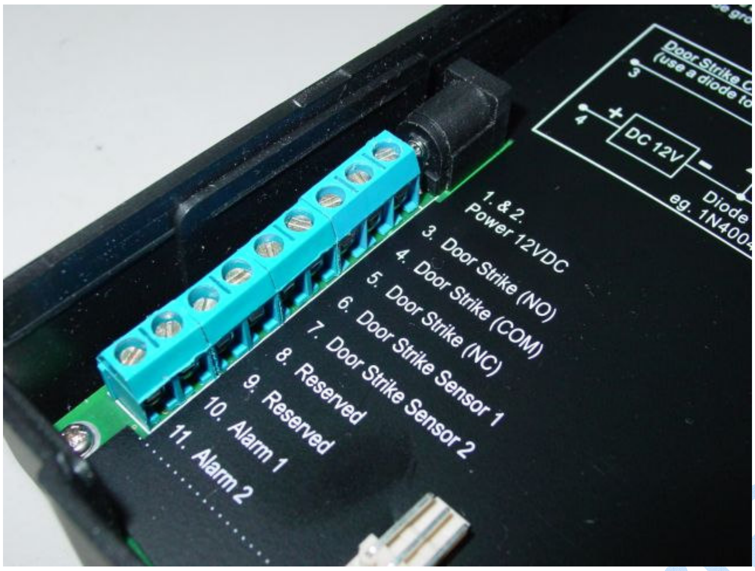
- Allow adequate air circulation to prevent internal heat buildup.
- Do not install the product next to heat-emitting sources, or in a place subject to direct sunlight and excessive dust.

1.4. **Important** Mounting the Metal Back Panel

The iGuard comes with a metal panel for mounting on the wall. ***The panel must be grounded***. By doing so, the static electricity that users emit can be discharged easily to the ground, which would improve the fingerprint images of users.

1.5. Connections - Power & external controls

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



Power (12V DC):

Terminals #1 (ground) & #2 (+12V). The power requirement is 12V DC, 150mA (idle), 500mA (peak).

Door Strike (Terminal 3 - 5):

(3 - 4 Normal Open, 4 - 5 Normal Close). These terminals are connected directly to the internal relay, rating at 12V / 1A. If the door strike is within this current limit, it can be directly connected to these terminals. If the system is used solely for Time Attendance System, these terminals can be left disconnected.

Door Sensor (optional):

Terminals #6 & #7. It provides iGuard the current status of the door (open / close). If the door is left open for over 10 seconds, iGuard will generate beep sounds to alert others.

External Alarm (optional):

Terminals #10 & #11. This is used for the optional external alarm. If the case of the device is forced open during operation (such as a break-in), an internal sensor will trigger this connection, and it will sound the external alarm.

External Relay (optional):

Switch on the right side. To make use of the external relay, you need to connect a two pin connector to the board of iGuard and then connect it back to the external relay. This controls the door strike from within the premises, heightening security and preventing break-ins.

1.6. Connections - Corporate Network

You can connect iGuard directly to your corporate computer network via standard RJ-45 cabling & TCP/IP protocols. By connecting it to the network, you can manage & monitor the unit via any standard web browser, such as Microsoft Internet Explorer & Netscape Navigator.

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

Power-up

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

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

After about 10 sec., the device will load the system program…	`iGuard System`
	`Loading...`

After loading the system program, iGuard will enter the standby mode and is now ready to use.	`Monday 30 13:49`
	`ID#:`

2. CONFIGURATION

2.1. Setting the date and time

You need to enter the date and time so that iGuard can time stamp all the access & time attendance records. Follow these steps to set the system date and time: -

Description	***LCD Display***
While in Standby Mode, press the **Func** key to enter the Setup Menu. You will be prompted to enter the Administrator Password as shown.	`Enter Password: _`

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

Press the **Func** key to continue. The setup menu will scroll down slowly as shown.	`Press 1:`
	`Add/Update ID`
	:
	`Press 5: System`
	`Configuration …`

Enter **5** to select the **System Configuration** menu. The current date is displayed. If necessary, enter the new date and then press the **Func** key to continue.	`Date (M/D/Y):`
	`08/30/1999`

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):`
	`13:45:23`

The system will then ask for the Terminal ID. The Terminal ID is used to identify the iGuard in your network, especially if you have installed more than one *(to be continued in the next section)*.	`Terminal ID:`

Note:

iGuard can keep the date & time running without power for approximately two days. Also, there is a software tool for users to synchronize the clock of the iGuard device with the desktop PC (iSetClock.exe), which can be downloaded freely at the website.

2.2. Setting the Network & TCP/IP address

You can connect iGuard directly to your corporate network. To do so, you would need to assign a device name & an IP address to the product. It is possible to use the DHCP server in your network to dynamically assign the IP address, but it is suggested to assign a static IP address to the product to avoid problems.

The following procedures show you how to assign the name, the IP addresses, and other related settings. Collect all the information before proceeding.

Description	***LCD Display***

While in Standby Mode, press the **Func** key to enter the Setup Menu. You will be prompted to enter the Administrator Password (default:. 123) as shown.	`Enter Password:`
	`_`

Enter **5** to select the **System Configuration** menu.	`Press 1: Add/Update ID`
	:
	`Press 5: System Configuration …`

Pressing the **Func** key until you see "DHCP/Static IP"	
Press **Func** key to continue, and then press **1** to select DHCP or **2** to select Static IP.	`DHCP/Static IP (1/2)? Static`

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. Enter the static IP address assigned to the device (e.g., 192.168.1.123).**Note: Please configure the IP according to your corporate network.**	`IP Address:`
	`192.168.001.123`

Press **Func** key to continue. Enter the sub-net mask here (e.g., 255.255.255.0).	`Subnetmask:`
	`255.255.255.000`

Press **Func** key to continue. Enter the address of the Default Gateway (e.g., 192.168.0.200).	`DefaultGateway:`
	`192.168.000.200`

Press **Func** key to continue. Enter the address of the Domain Name Server (e.g., 192.168.0.200). Make sure	`DNS:`
	`192.168.000.200`

that the IP address of all units are unique. **(Warning: IP addresses that are not unique will cause network error and the iGuard would not function.**	
Press **Func** key to continue. You will be asked if the device is a *Master* or *Slave* device (1/2)? If you have only one unit of iGuard, choose (1) Master. If you have more than one units of iGuard, you have to decide which is the Master and which are the Slave(s). If you choose (2) Slave, the system will ask you to provide the Master IP Address, key in, default: 192.168.0.100. Please also read the section about Master and Slave mode.	Master/Slave (1/2)? Master
iGuard FPS110 can be configured as Master or Slave device. Select one and then press **Func** key. The system will reset itself and then return to Standby Mode.	Mon Aug 30 13:46 ID #:_

2.3. The Company Code

The *Company Code* is introduced for the units with the Smart Card option. The Company Code is used to make sure that the unit only reads the smart cards issued by the company. For example, if the Company Code of the unit is 1234, it only reads the smart cards with the same Company Code, and will ignore the cards with different company code.

All the units in the same company must have the same company code, and this company code should be kept confidentially. The company code is set up in the web page Administration - Terminal Setup via the web browser.

Please note that in the Master / Slave configuration, all the Slave units should have the same company code as the Master unit.

2.4. Setting the Administrator Password & Access Password

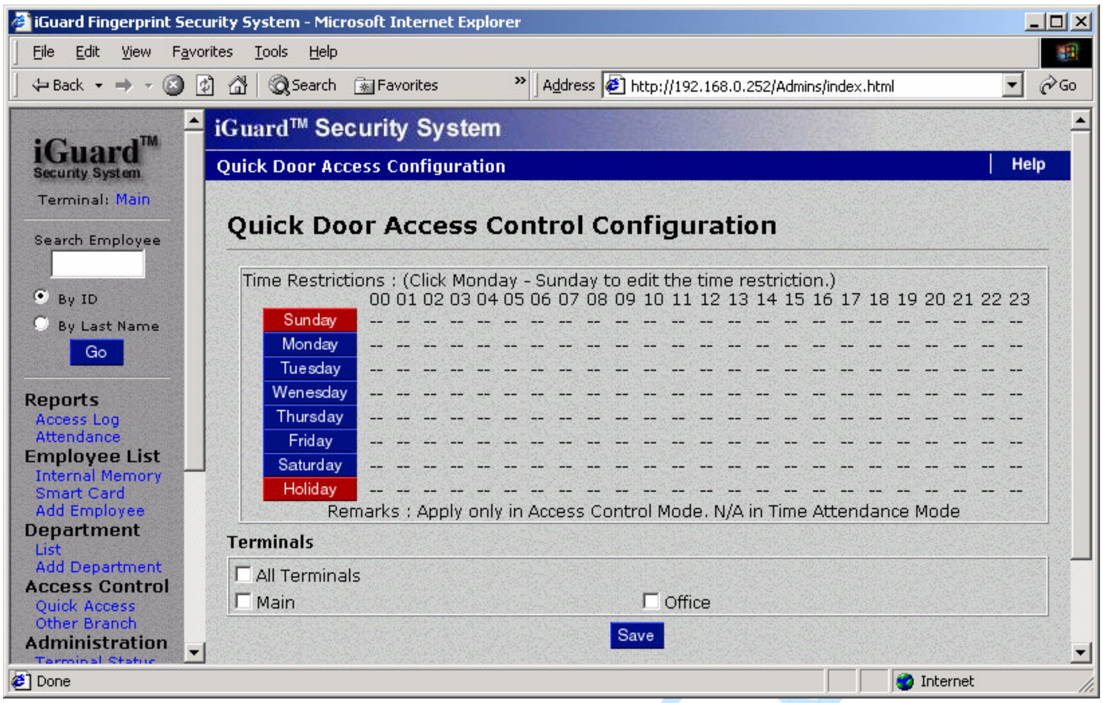
iGuard has three *"global"* passwords[1]. The ***System Administrator Password*** is used to access the system menu and to configure the system (such as accessing the setup menu in the last example). The ***User Administrator Password*** is used to manage the user accounts. **The *Door Access Password*** is used to release the door strike in Quick Access option.

Follow these steps to assign & edit the three passwords:

Description	***LCD Display***
While in Standby Mode, press the **Func** key to enter the Setup Menu. Enter the System Administrator Password (default 123) and press **Func** key, then press **6** to select "Set Password" menu. The menu "Admin/Personal (1/2)?" will display. Press **1** to select Administrator password.	System Admin: 123_
Press the to erase the old password, and enter the new password (e.g., AB456). The field size limit for individual passwords is 10 digits, from 0-9 and A/B.	System Admin: AB456_
Press the **Func** key to accept the new System Administrator Password. You will then be prompted for the User Administrator Password as shown.	User Admin: _
Enter the new User Administrator Password (e.g., 7890BA).	User Admin: 7890BA_
Press the **Func** key to accept the new User Administrator Password. You will then be prompted for the Door Access Password as shown.	Door Access: _
Enter the new Door Access Password (e.g., 9394AB709). It is suggested to use a long and hard-to-guess password.	Door Access: 9394AB709_
Press **Func** to return to the standby mode.	Mon Aug 30 13:49 ID #:_

Note:

You must enable the Door Access Password before it can be used, by specifying the corresponding authorized time and terminals. It is disabled in the factory settings. The only way to enable it is via the Internet browser (discussed in later sections), under the "*Quick Access*" page as follows: -



Quick Door Access Control Configuration

Time Restrictions : (Click Monday - Sunday to edit the time restriction.)

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sunday	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Monday	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Tuesday	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Wenesday	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Thursday	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Friday	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Saturday	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Holiday	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

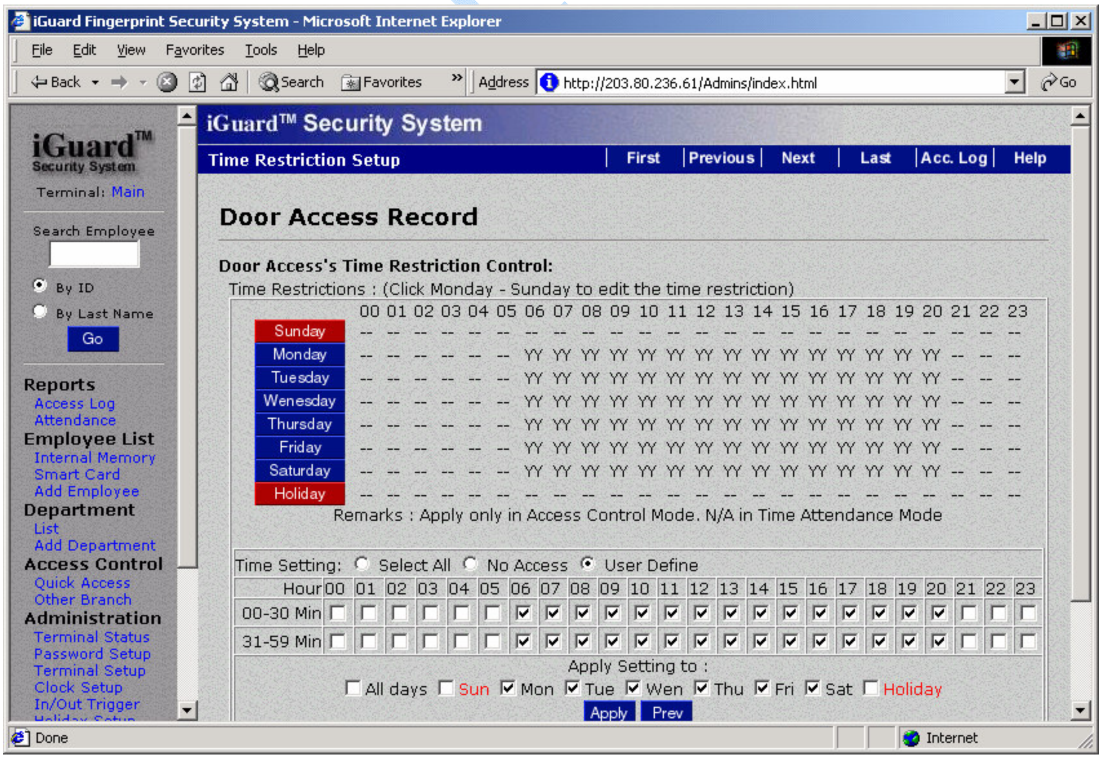
Remarks : Apply only in Access Control Mode. N/A in Time Attendance Mode

Terminals

□ All Terminals

□ Main □ Office

As shown in the figure above, there is no authorized time assigned in the default setting, and none of the terminals is selected neither. You must specify the authorized period by first clicking on any one of the Day buttons (i.e., Sunday to Saturday and Holiday buttons), then select the desire time period (in 30-min interval). The following figure shows a typical setting: -



Door Access Record

Door Access's Time Restriction Control:

Time Restrictions : (Click Monday - Sunday to edit the time restriction)

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sunday	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Monday	--	--	--	--	--	--	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	--	--	--
Tuesday	--	--	--	--	--	--	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	--	--	--
Wenesday	--	--	--	--	--	--	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	--	--	--
Thursday	--	--	--	--	--	--	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	--	--	--
Friday	--	--	--	--	--	--	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	--	--	--
Saturday	--	--	--	--	--	--	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	--	--	--
Holiday	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Remarks : Apply only in Access Control Mode. N/A in Time Attendance Mode

Time Setting: ○ Select All ○ No Access ● User Define

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
00-30 Min	□	□	□	□	□	□	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	□	□	□
31-59 Min	□	□	□	□	□	□	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	□	□	□

Apply Setting to :

□ All days □ Sun ☑ Mon ☑ Tue ☑ Wen ☑ Thu ☑ Fri ☑ Sat □ Holiday

After specifying the authorized time and terminals, you can gain access using the Door Access Password, and it is illustrated in the following steps: -

Description	***LCD Display***
Press the **Func** key while in the Standby Mode. You will then be asked to enter the password.	Enter Password: _
Enter the Door Access Password (such as 9394AB709). The password is shown as astride for security reason.	Enter Password : *********
Press the **Func** key again to proceed. If the password is right, iGuard will release the door strike, and will return to the Standby Mode.	Mon Aug 30 13:49 ID #:_

More details about using the Internet browser will be discussed in later sections.

[1] You should not confuse these Global Passwords with the Personal Password, which can be assigned uniquely to each individual. More details about the Personal Password will be discussed in later sections.

3. BASIC OPERATION

3.1. ENROLLMENT

3.1.1. Enrollment with fingerprint

Fingerprint enrollment is to register a fingerprint template for later recognition. A good enrollment is crucial for all reliable fingerprint recognition systems, including the iGuard.

iGuard takes advantage of the advanced DFX (Difficult Fingerprint Extraction) technology (originally developed by Bell Labs USA), which works accurately with most people's fingerprint images. iGuard can achieve an exceptionally low false-rejection-rate of less than 1 %.

However, as individuals, our hands have different levels of moisture. In some cases, iGuard may have difficulty in recognizing specific users' fingerprint images, most commonly, people with dry skin. The problem is more noticeable during the enrollment process since the sensor requires a more accurate and higher quality fingerprint image than the normal verification process. The easiest way to get around this problem is to apply a small amount of moisturizing lotion on our fingers during the enrollment process. This step is only required in the enrollment stage, and will not be needed in daily verification process.

In the case of poor fingerprint quality or dry finger, iGuard will ask you if you want to lower the matching security. A low security level will bring more convenience to the user but with a minor sacrifice of security. We recommend to choose low security only for time attendance application.

Each person must register two fingers: one as the primary and the other one as the secondary. In case that the primary finger is not suitable for verification such as when the finger is hurt, the person can use his/her secondary finger for the authentication process.

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

It is suggested to use your two thumbs as your primary and secondary fingers. It is because your thumbs are usually bigger and can cover the scanner area better.

IMPORTANT: During the enrollment process, you must position the center of your fingerprint of your 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.

The following steps show you how to register the user's fingerprint template:

Description	***LCD Display***
While in standby mode, press the **Func** key to enter the Setup Menu. Enter the Administrator Password (default 123) and press **Func** key, then press **1** to select "Add /Update ID" menu. Press **1** to input fingerprint.	By Finger/Passwd (1/2)? Enter ID # and scan 1st Finger
Enter the user ID # (e.g. A01). The ID can be of any length from 1 character to 8 characters.	Enter ID# A01_
Press the **Func** key to confirm the ID #. The device now begins to capture the 1st image of the primary finger. The horizontal bar on the second line indicates the quality of the image. Lift the sensor shutter with your right-hand thumb and place it firmly on the sensor until the quality bar reaches the right end. You may need to move and rotate the thumb a little bit to achieve the required quality.	Scanning 1 of 3... : : Scanning 1 of 3...
After the quality bar reaches the right end, you will be asked to remove the finger from the sensor.	Analyzing. Pls remove finger...
When the device detects that you have removed the finger, it will ask you to place it back again for the 2nd image.	Press Func to scan 2 of 3
Press the **Func** key and repeat the same procedure, and you will be asked to scan the 3rd time of the same primary finger.	Press Func to scan 3 of 3
Press the **Func** key again and repeat the procedure for the third time. You will then be asked to scan the secondary finger.	Press Func to scan 2nd Finger

Press the **Func** key, and repeat the above steps to scan the left-hand thumb three times again. If all the images are OK, you will see the acknowledge message "ID: A01 Added OK!" momentary, then the device is ready for next enrollment.	`ID: A01 Added OK!`
	:
	:
	`Enter ID # and`
	`scan 1st Finger`

Press ← to return to the standby mode.	`Mon 30 Aug 12:00`
	`ID #:_`

In the case of dry finger (poor fingerprint image), it will warn you for dry finger. You can either wet your finger with lotion and try again, or continue.	`Scanning 1 of 3`
	`=== Too Dry !===`

If continue with dry finger, at the end, it will prompt you if you want to set security to low2. We recommend to choose low security only for time attendance application.	`Set Security to`
	`Low2 yes(1)/No(2)?`

3.1.2. Enabling Automatch

This feature enables the device to identify a person without requiring the user to first enter his/her user ID, and must be turn on via the Internet browser, as described in the next section. All that needs to be done is to present your enrolled finger to the sensor and wait for it to match your fingerprint template with stored templates. Once a match is made, the door opens and the system will then return to the standby mode.

The maximum number of users allowed to access the iGuard using automatch is recommended to be limited to **30** users. This is due to the fact that the iGuard would require some time to process the fingerprint and then search for it across ALL the database stored on your iGuard. It is therefore recommended that the automatch feature is left for top management and the rest of staff can use ID plus Fingerprint for access. Also, user with poor fingerprint quality shall not use automatch.

3.1.3. Enrollment with Smart Card (for Models with Smart Card reader)

The user has to be created prior to use this function either the fingerprint is enrolled or the password is added. After the enrollment procedure, the user ID and the fingerprint template is stored in the internal memory.

Please note that only one (the primary) fingerprint template is stored on the smart card.

The following steps illustrate how to write the user information to a Smart Card:-

Description	***LCD Display***
While in the standby mode, press the **Func** key to enter the Setup Menu. Enter the Administrator Password (default 123) and press **Func** key, then press **9** to select "Issue/Import Card" menu. Press **1** to issue Smart Card.	**Enter ID #: _**
Enter the ID # you want to write to the Smart Card (e.g., A01).	**Enter ID #: A01_**
Press the **Func** key to confirm. You will then be asked to present the Smart Card.	**Waiting for** **SmartCard...**
Present a Smart Card near the keypad. The unit will then write the user information to the card.	**Writing....**
After writing to the card, you will be asked whether or not to remove the user's fingerprint information from the internal memory. It is recommended not to remove user fingerprint information from memory.	**Remove Fingerprint** **Yes(1)/No(2)?**
The unit will prompt for another ID.	**Enter ID #: _**
Press <-- key once or wait till time out, the unit will return to the standby mode.	**Mon Aug 30 12:00** **ID #:_**

Please note that the above procedure will overwrite all the existing information stored in the Smart Card.

3.1.4. Registering an existing Smart Card

The first time a user accesses a remote unit in a remote branch with this smart card, the user must register the Card to this unit. In addition, after registering the system administrator must also assign the departments the user belongs to, to grant the user the access rights required. After that, the user can use his/her card to access the remote unit same as the one in his/her own branch.

The registration procedure reads the user information from the Smart Card, and stores the information in the Smart Card Memory of the internal user database.

The procedure is done via the **Function 0** in the Setup menu, and is illustrated in the following steps:-

Description	***LCD Display***
While in the standby mode, press the **Func** key to enter the Setup Menu. Enter the Administrator Password (default 123) and press **Func** key, then press **9** to select "Issue/import Card" menu. Press **2** to import Smart Card.	`Enter ID #: _`

You will then be asked to present the Smart Card.	`Waiting for`
	`Smart Card...`

Present a Smart Card near the keypad. The unit will then write the user information to the card.	`Writing....`

3.1.5. Verification with Fingerprint

The device 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***

While in the standby mode, key in the user ID number (e.g., A01).	`Mon Aug 30 13:49`
	`A01_`

Lift the shutter and place either your primary	`Scanning... A01_`

finger (right-hand thumb) or your secondary finger (left-hand thumb) on the sensor. You should place the finger the same way as you did during the enrollment procedure. The device will automatically start scanning when the sensor shutter is lifted all the way up.	: : Verifying...
If you are authenticated, the device will open the door, and will return to the standby mode.	A01 Authorized! : : Mon Aug 30 13:49 ID #:_

Note: there is another feature called *Auto-Match*, which allows the user to access the device without the need to enter his/her ID first.

3.1.6. Verification with Automatch

The automatch feature allows users to get authorized without inputting their user ID. This feature allows top management to enter the premises without having to enter their ID, enable them quicker access and giving them high convenience.

Description	***LCD Display***
While in Standby Mode, place either your primary or secondary finger on the sensor by lifting the shutter. The device will automatically start scanning when the sensor shutter is lifted all the way up	Mon Aug 30 13:49 == Automatch !== : : Mon Aug 30 13:49 Verifying...
If you are authorized, the device will open the door, and will return to the standby mode.	Mon Aug 30 13:49 Authorized !

3.1.7. Verification with Smart Card

The procedure for authenticating using smart card is simple and straightforward, and it is illustrated in the following steps:-

Description	***LCD Display***
While in standby mode, present the smart card near the keypad. The unit will read the data stored in the card, and if the card is valid (i.e., it is not a blank card and with the correct company code), you will be asked to scan your finger.	**Jacky Hui** **Waiting Finger**
The fingerprint image matches the data stored in the card, the user is authenticated. The unit will return to the standby mode, and it is ready for the next card.	**Jacky Hui** **Authorized**

3.1.8. Verification with Password

Description	***LCD Display***
While in standby mode, key in the user ID number (e.g., A01).	**Mon Aug 30 13:49** **A01_ IN**
Instead of lifting the shutter and placing the finger on the sensor, press the **Func** key.	**Your Password:**
Enter the personal password (e.g., 123456)	**Your Password:** **********
Press **Func** key again to confirm. If the personal password is correct, the person is authenticated and the message will appear.	**A01** **Authorized**

3.1.9. Suspending Resuming User

You can temporary suspend a user ID. This is useful if you want to temporary stop a user from getting into your business premises, and you may want to resume his access right later on. This is done via the function “Inactive ID" in the function menu, and it is illustrated in the following steps: -

Description	***LCD Display***
While in Standby Mode, press the **Func** key to enter the Setup Menu. Enter the Administrator Password (default 123) and press **Func** key, then press **2** to select “Inactive ID" menu.	**Enter ID:**
Enter the ID # you want to suspend (e.g., A01).	**Enter ID: A01**
Press the **Func** key to confirm. The ID # is suspended, and the user can no longer be authenticated. The system will return to the standby mode.	**ID A01:** **Inactivated !**

3.2. OTHER FUNCTIONS

3.2.1. Deleting ID

You can permanently delete a user using similar procedure as described above, and it is illustrated as follows: -

Description	***LCD Display***
While in standby mode, press the **Func** key to enter the Setup Menu. Enter the Administrator Password (default 123) and press **Func** key, then press **4** to select "Delete ID" menu	**ID to Delete:**
Enter the ID # you want to delete (e.g., A01).	**ID to Delete:** **A01**
Press the **Func** key to confirm. The ID # is deleted, and the user can no longer get access. The system will return to the standby mode.	**ID #A01** **Deleted!**

Note:
Once an employee ID is deleted, all the information associated with the employee ID, such as the fingerprint data and the access rights, will also be permanently deleted. You must re-enroll the employee if necessary.

3.2.2. Resetting the device

The device can be turned off easily by just simply turning the power off. However, there is a very small chance that the unit is in the process of accessing and updating the internal flash memory at the moment when the power is discontinued. This may result in data loss.

The safe way to turn the unit off is to do a proper shut down by accessing **Func 7** in the menu. You can also reset the user database and the access log with this function. In addition, you can reset all the 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.).

3.2.3. Emergency Procedures

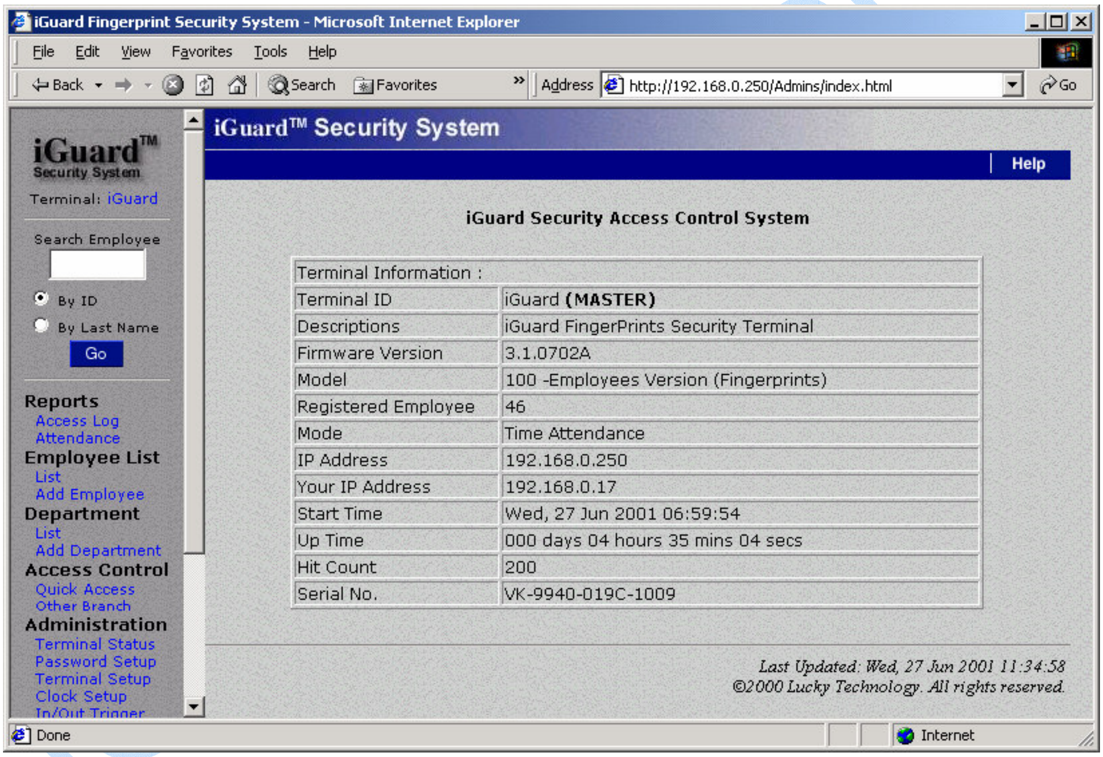
This feature has been added as a safety precaution, just in case your iGuard fails to respond to you and does not unlock the door as instructed. While in the standby mode, press the **Func** key to enter the Setup Mode. Enter your Administrator Password (default 123) and press the **Func** key once again. Then, press **B** to unlock the door manually.

4. ADMINISTRATION

4.1. Using Web Brower

The built-in Web Server in each iGuard device allows you to use the popular Internet Browser software to manage and configure the device, and to access the records of these devices. You can use the popular Microsoft Internet Explorer or Netscape Navigator software running under different platform such as Windows 98, Windows 2000, Windows Me, Apple Macintosh, Linux and Unix machines.

Once connected to your corporate computer network, you can access the device by specifying the IP address (eg., http://192.168.0.100). This is the IP address assigned to the device during the setup procedure. The following screen will be displayed: -



iGuard Security Access Control System

Terminal Information :	
Terminal ID	iGuard **(MASTER)**
Descriptions	iGuard FingerPrints Security Terminal
Firmware Version	3.1.0702A
Model	100 -Employees Version (Fingerprints)
Registered Employee	46
Mode	Time Attendance
IP Address	192.168.0.250
Your IP Address	192.168.0.17
Start Time	Wed, 27 Jun 2001 06:59:54
Up Time	000 days 04 hours 35 mins 04 secs
Hit Count	200
Serial No.	VK-9940-019C-1009

Last Updated: Wed, 27 Jun 2001 11:34:58
©2000 Lucky Technology. All rights reserved.

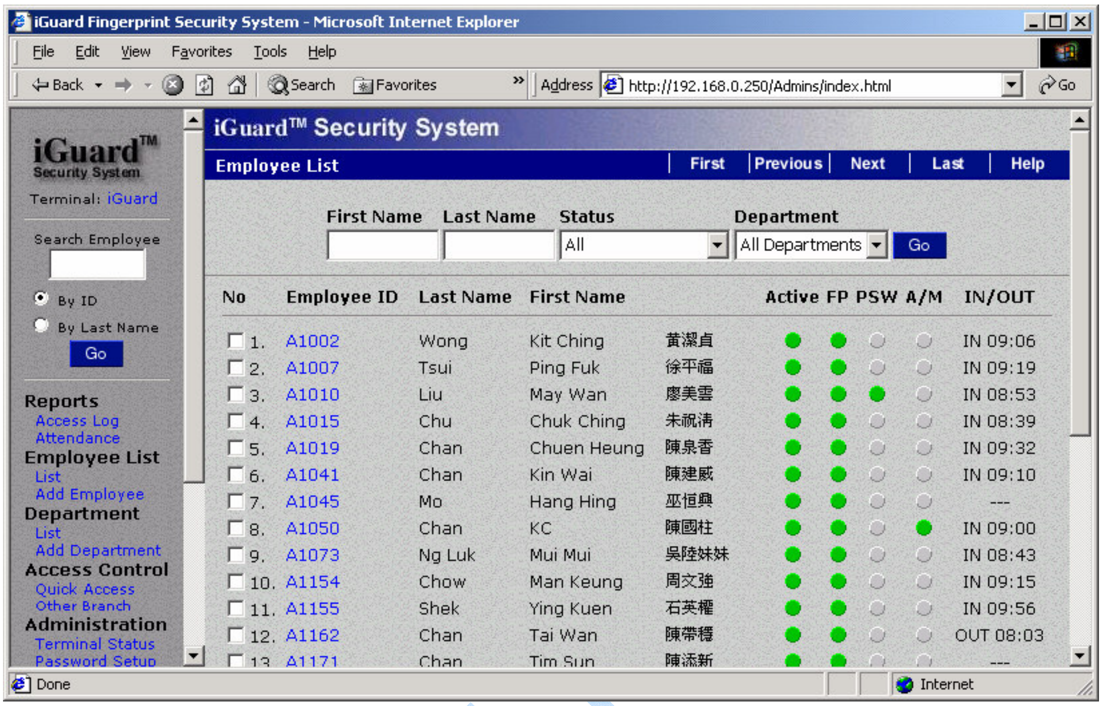
The iGuard's home page is divided into left and right panels. You can select different functions in the left panel, and the right panel will display the corresponding results.

Note: The home page of your iGuard may be different from the one shown above depending on the model you have.

Each item in the left panel corresponds to different pages in the right panel, and will be discussed in the following sections.

4.2. Employee List

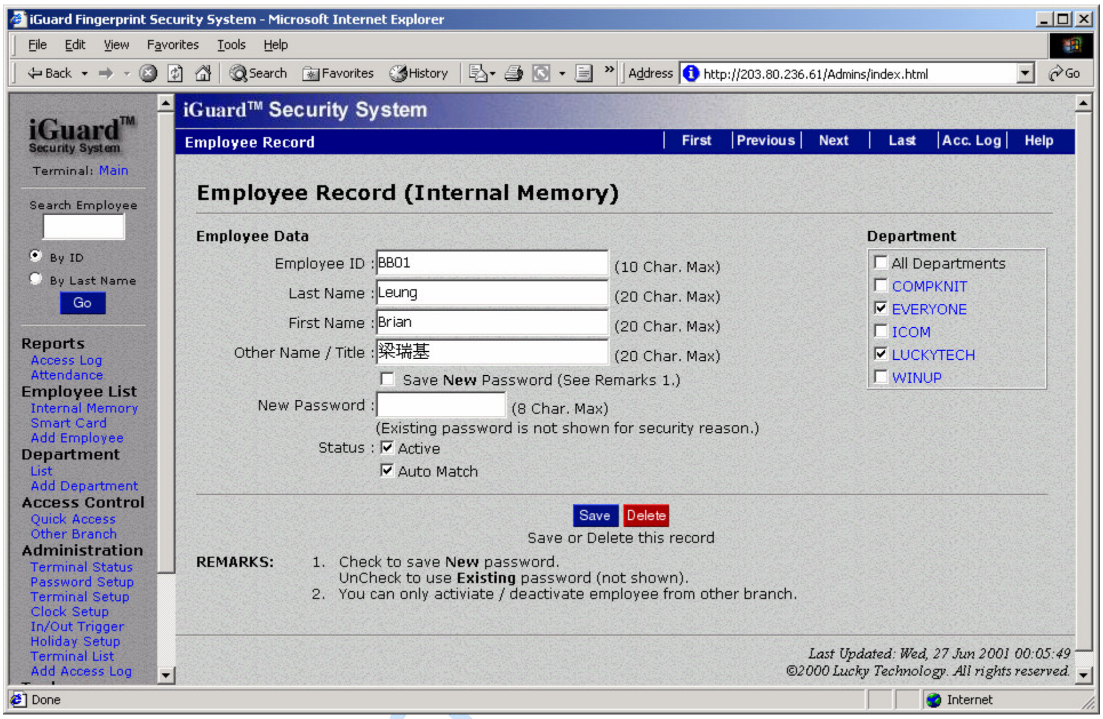
Click *Employee List,* it will show the complete list of employees.



No	Employee ID	Last Name	First Name		Active	FP	PSW	A/M	IN/OUT
□ 1.	A1002	Wong	Kit Ching	黃潔貞	●	●	○	○	IN 09:06
□ 2.	A1007	Tsui	Ping Fuk	徐平福	●	●	○	○	IN 09:19
□ 3.	A1010	Liu	May Wan	廖美雲	●	●	●	○	IN 08:53
□ 4.	A1015	Chu	Chuk Ching	朱祝清	●	●	○	○	IN 08:39
□ 5.	A1019	Chan	Chuen Heung	陳泉香	●	●	○	○	IN 09:32
□ 6.	A1041	Chan	Kin Wai	陳建威	●	●	○	○	IN 09:10
□ 7.	A1045	Mo	Hang Hing	巫恒興	●	●	○	○	---
□ 8.	A1050	Chan	KC	陳國柱	●	●	○	●	IN 09:00
□ 9.	A1073	Ng Luk	Mui Mui	吳陸妹妹	●	●	○	○	IN 08:43
□ 10.	A1154	Chow	Man Keung	周文強	●	●	○	○	IN 09:15
□ 11.	A1155	Shek	Ying Kuen	石英權	●	●	○	○	IN 09:56
□ 12.	A1162	Chan	Tai Wan	陳帶穩	●	●	○	○	OUT 08:03
□ 13.	A1171	Chan	Tim Sun	陳添新	●	●	○	○	---

4.3. Employee List - Add Employee

Normally a new employee is added in the enrollment process, as already discussed in the "Basic Operation - Enrollment" section. However, you can also add an employee in the *Add Employee* page. Please note that even though an employee is added on this page, the employee is still required to register his/her fingerprint image physically at the device before he/she can authenticate with the device.



Employee Record (Internal Memory)

Employee Data

Employee ID : BB01 (10 Char. Max)
Last Name : Leung (20 Char. Max)
First Name : Brian (20 Char. Max)
Other Name / Title : 梁瑞基 (20 Char. Max)
□ Save **New** Password (See Remarks 1.)
New Password : (8 Char. Max)
(Existing password is not shown for security reason.)
Status : ☑ Active
☑ Auto Match

Department
□ All Departments
□ COMPKNIT
☑ EVERYONE
□ ICOM
☑ LUCKYTECH
□ WINUP

Save Delete
Save or Delete this record

REMARKS:
1. Check to save **New** password.
UnCheck to use **Existing** password (not shown).
2. You can only activiate / deactivate employee from other branch.

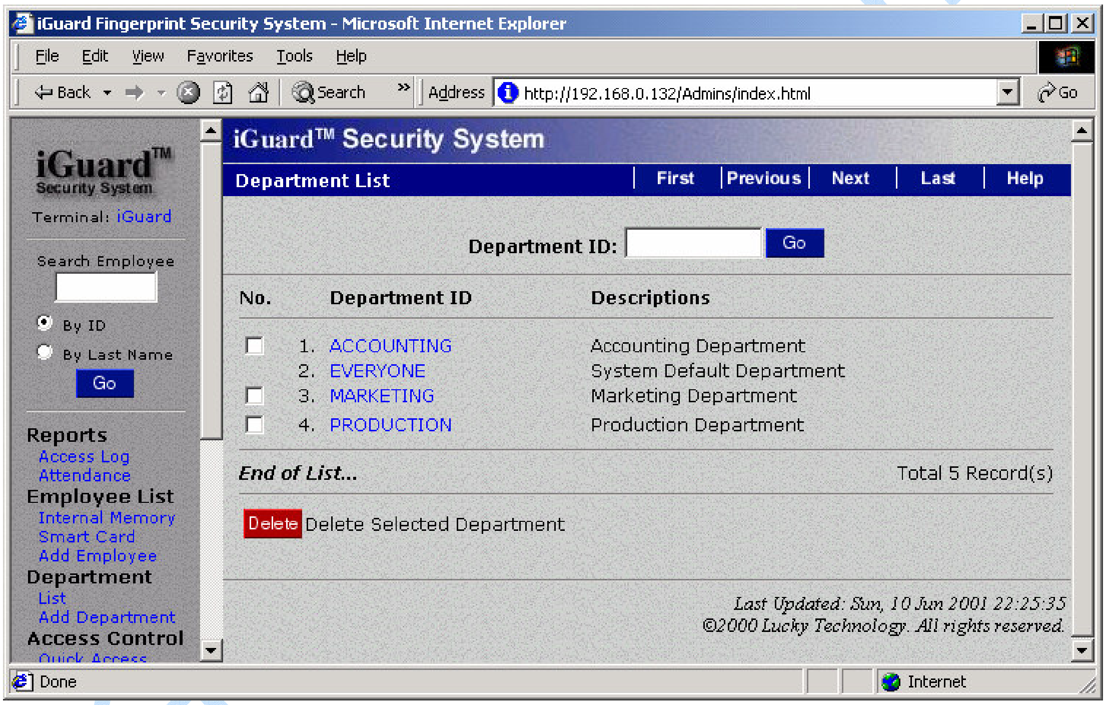
Last Updated: Wed, 27 Jun 2001 00:05:49
©2000 Lucky Technology. All rights reserved.

4.4. Department - List

One of the purposes of setting up departments is to divide the employees into different groups. Each department has its own authorized access time. For example, you can assign the authorized time period for the Marketing Department from 9:00 am to 6:00 pm, and all the members in the Marketing Department can access the device only within he specified time period.

The maximum number of departments is 32.

The Department List page is shown as follows:



http://192.168.0.132/Admins/index.html

iGuard™ Security System

Department List

Department ID: Go

	No.	Department ID	Descriptions
□	1.	ACCOUNTING	Accounting Department
	2.	EVERYONE	System Default Department
□	3.	MARKETING	Marketing Department
□	4.	PRODUCTION	Production Department

End of List... Total 5 Record(s)

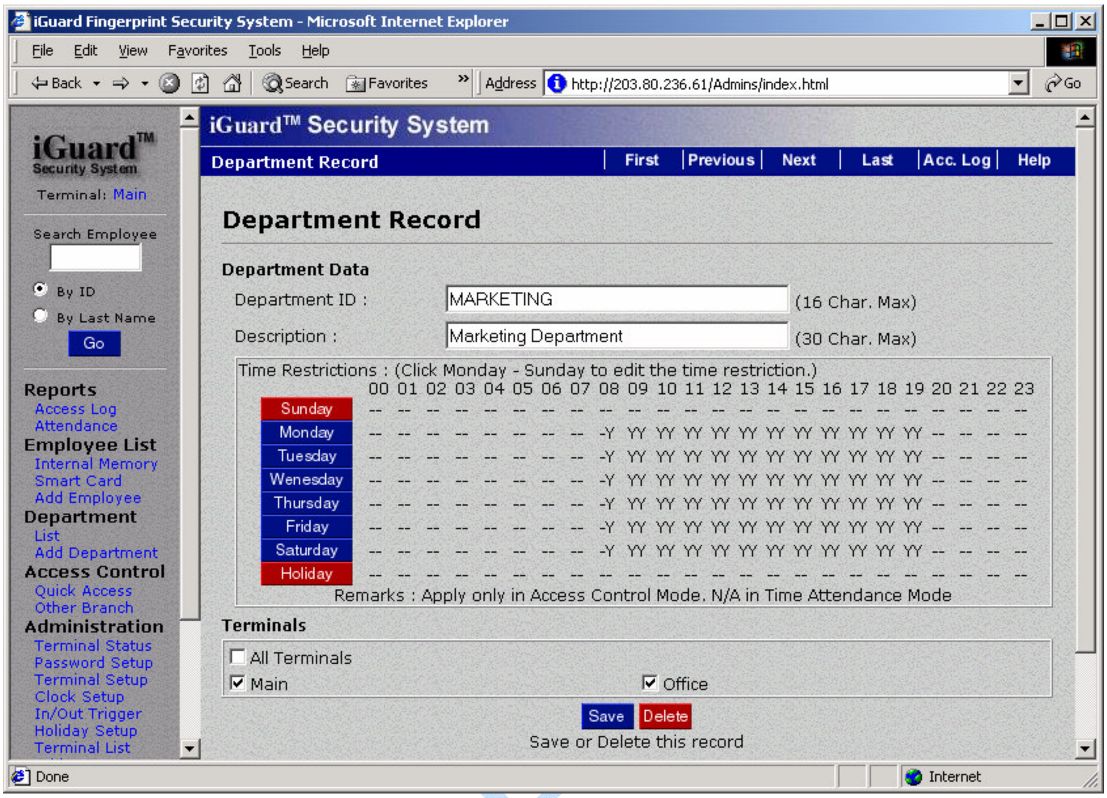
Delete Delete Selected Department

Last Updated: Sun, 10 Jun 2001 22:25:35
©2000 Lucky Technology. All rights reserved.

This page lists all the departments available. The EVERYONE department is the default department and cannot be deleted. When a new employee is added, this new employee is automatically added to the EVERYONE member list. You can edit the time restriction of this default department (discussed in next section), and you can also remove the employee from the department.

You can delete a single department or a group of departments by first checking the checkbox of the departments, and press the **Delete** button at the bottom. Please note that you cannot delete the default department EVERYONE.

To edit the authorized time period of a particular department, click on the department ID in the above page (e.g., MARKETING). The following page will appear: -



Department Record

Department Data

Department ID : MARKETING (16 Char. Max)

Description : Marketing Department (30 Char. Max)

Time Restrictions : (Click Monday - Sunday to edit the time restriction.)

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sunday	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Monday	--	--	--	--	--	--	--	--	-Y	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	--	--	--	--
Tuesday	--	--	--	--	--	--	--	--	-Y	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	--	--	--	--
Wenesday	--	--	--	--	--	--	--	--	-Y	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	--	--	--	--
Thursday	--	--	--	--	--	--	--	--	-Y	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	--	--	--	--
Friday	--	--	--	--	--	--	--	--	-Y	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	--	--	--	--
Saturday	--	--	--	--	--	--	--	--	-Y	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	--	--	--	--
Holiday	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Remarks : Apply only in Access Control Mode. N/A in Time Attendance Mode

Terminals

□ All Terminals
☑ Main ☑ Office

Save Delete

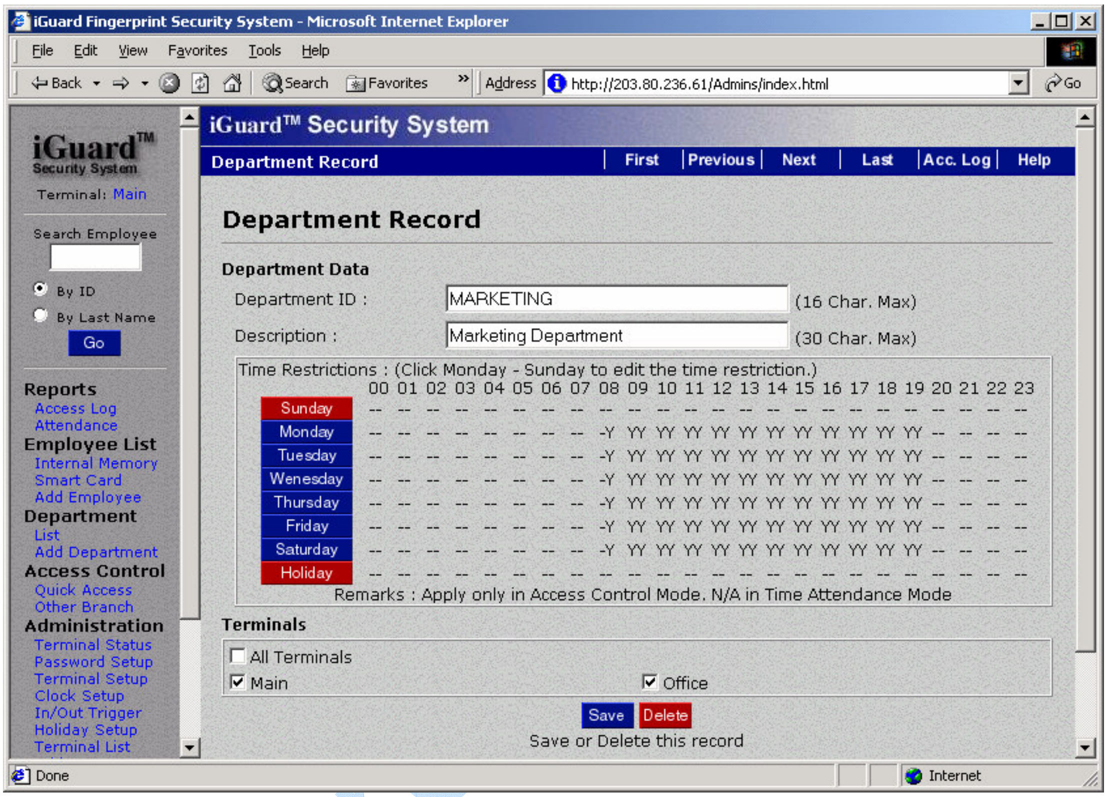
Save or Delete this record

The above page indicates that the authorized time period for the department Marketing is from 8:30 am to 7:59 pm, Monday to Saturday. As a result, all the members of this department can only be authenticated within this period.

You can edit the authorized time of a particular day (e.g., Monday) by clicking on the Monday button, and the web page in the next page will appear. You can select the authorized time period at the bottom of the page. If you want to select all the time slots, you can simply select the "Select All" checkbox above. You can also select the "All Days" checkbox to include all the days of the week.

4.5. Department - Add Department

To add a new department, click on the *Add Department* link on the left. It will display the following page. Please note that the maximum number of department allowed is 32.



Department Record

Department Data

Department ID : MARKETING (16 Char. Max)

Description : Marketing Department (30 Char. Max)

Time Restrictions : (Click Monday - Sunday to edit the time restriction.)

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sunday	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--
Monday	--	--	--	--	--	--	--	--	-Y	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	--	--	--	--
Tuesday	--	--	--	--	--	--	--	--	-Y	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	--	--	--	--
Wenesday	--	--	--	--	--	--	--	--	-Y	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	--	--	--	--
Thursday	--	--	--	--	--	--	--	--	-Y	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	--	--	--	--
Friday	--	--	--	--	--	--	--	--	-Y	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	--	--	--	--
Saturday	--	--	--	--	--	--	--	--	-Y	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	--	--	--	--
Holiday	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Remarks : Apply only in Access Control Mode. N/A in Time Attendance Mode

Terminals

□ All Terminals

☑ Main ☑ Office

Save Delete

Save or Delete this record

Enter the Department ID and Description in the above text boxes. After that, you should click on a day to set the *Time Restrictions* for employees to enter the premises.

If you wish to define the specific timings of access, under *Time Setting*, select "User Define". This will allow you to check the timings of access, which can be from 08:00 - 19:00. Then select the days you would want these changes to affect. For all days, check the "All Days" check box. For others, check the corresponding boxes of the days you wish these changes to effect.

After selecting the days, click "Apply" to save these settings.

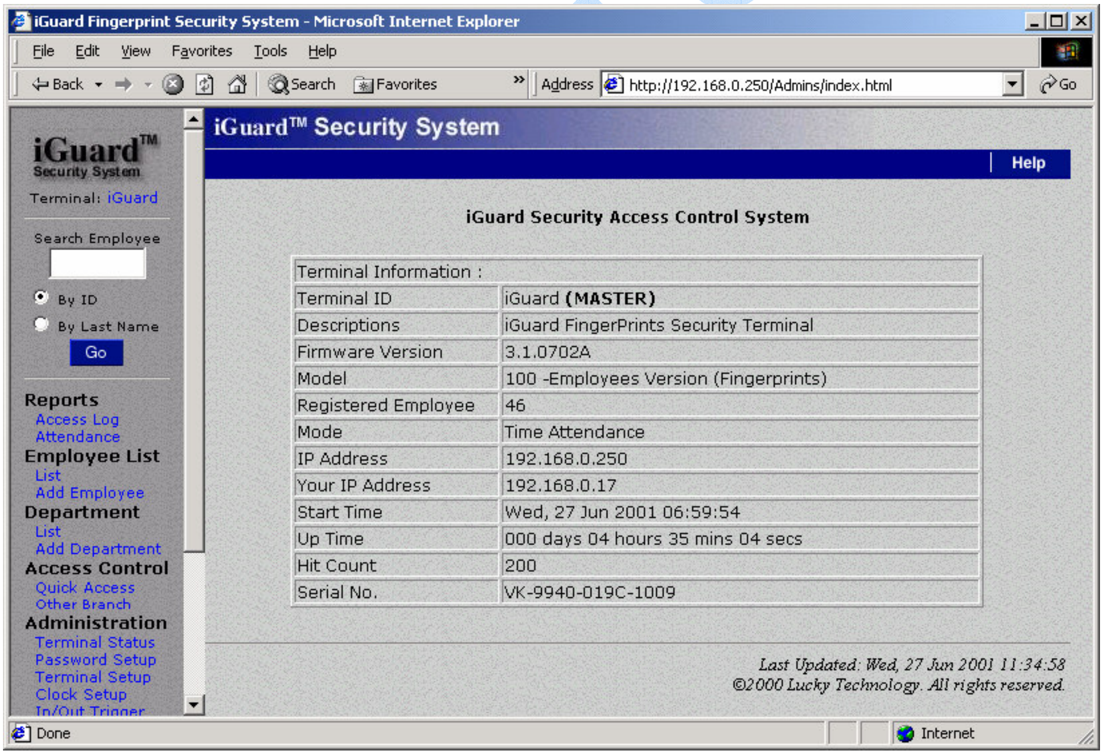
4.6. Access Control - Quick Access

Quick Access can be used for bypassing the fingerprint authentication process. The default setting does not allow you to use the Access Password (see **Administration - Password Setup**)or Smart Card (for Smart Card model) to by-pass the fingerprint authentication process.

The procedure for setting this page up is similar to the procedure for setting up the department. Once the current time is within the valid period, users can use the Access Password or Smart Card to enter the premises.

4.7. Administration - Terminal Status

This is the home page of the device. It shows the general information of the device, including the model, the number of registered users, the serial number of the unit, and more.



Address: http://192.168.0.250/Admins/index.html

Terminal: iGuard

● By ID
○ By Last Name

iGuard Security Access Control System

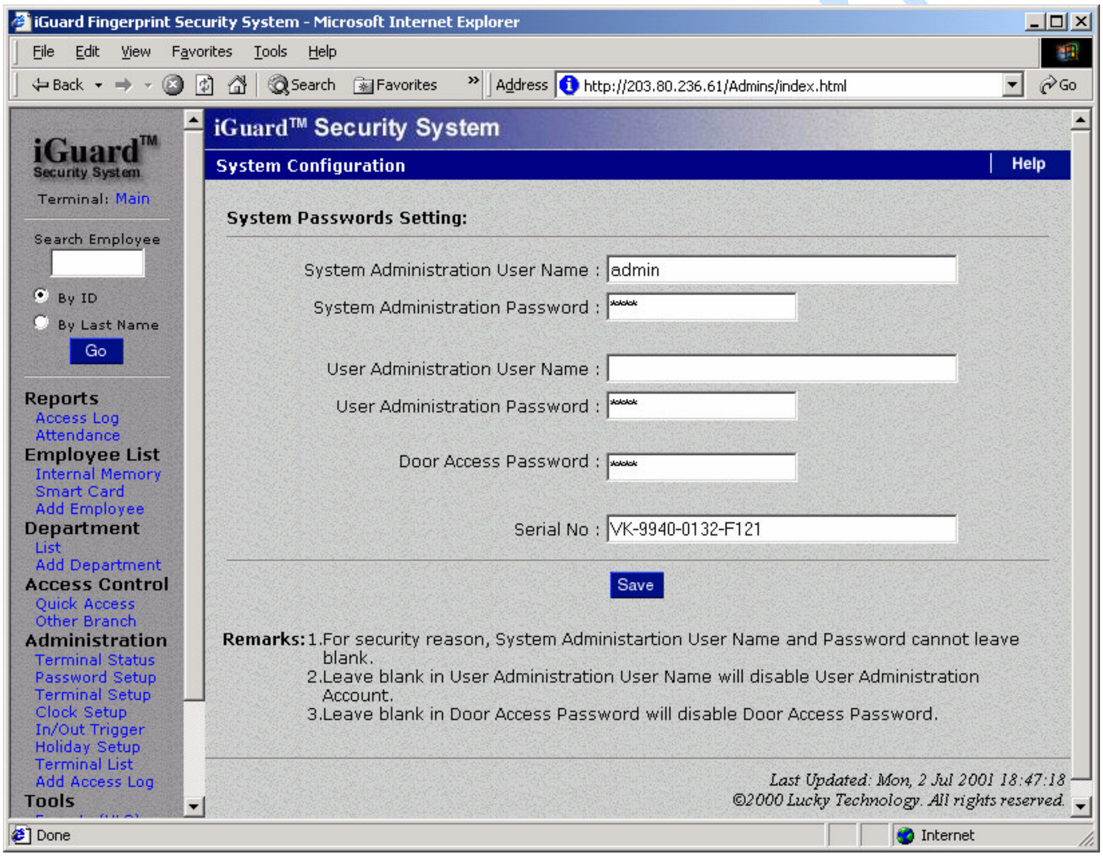
Terminal Information :	
Terminal ID	iGuard **(MASTER)**
Descriptions	iGuard FingerPrints Security Terminal
Firmware Version	3.1.0702A
Model	100 -Employees Version (Fingerprints)
Registered Employee	46
Mode	Time Attendance
IP Address	192.168.0.250
Your IP Address	192.168.0.17
Start Time	Wed, 27 Jun 2001 06:59:54
Up Time	000 days 04 hours 35 mins 04 secs
Hit Count	200
Serial No.	VK-9940-019C-1009

Last Updated: Wed, 27 Jun 2001 11:34:58
©2000 Lucky Technology. All rights reserved.

4.8. Administration - Password Setup

Setup the Administrator Passwords & the Door Access Password as follow:

- System Administration - This is the user name and password required to configure the system (such as setting up the IP address of the device), and to administrate the users' settings (such as adding and deleting users). The default name is **admin**, and the default password is **123**.
- User Administration - This is similar to the previous one, except that it cannot be used to configure the system. There is no default value.
- Door Access Password - This is the quick-access password for the *Quick Access* configuration. This is the common password that all the users use to open the door during the high-traffic period (such as during normal office hour), when high security is not necessary.



System Passwords Setting:

System Administration User Name : admin

System Administration Password : ****

User Administration User Name :

User Administration Password : ****

Door Access Password : ****

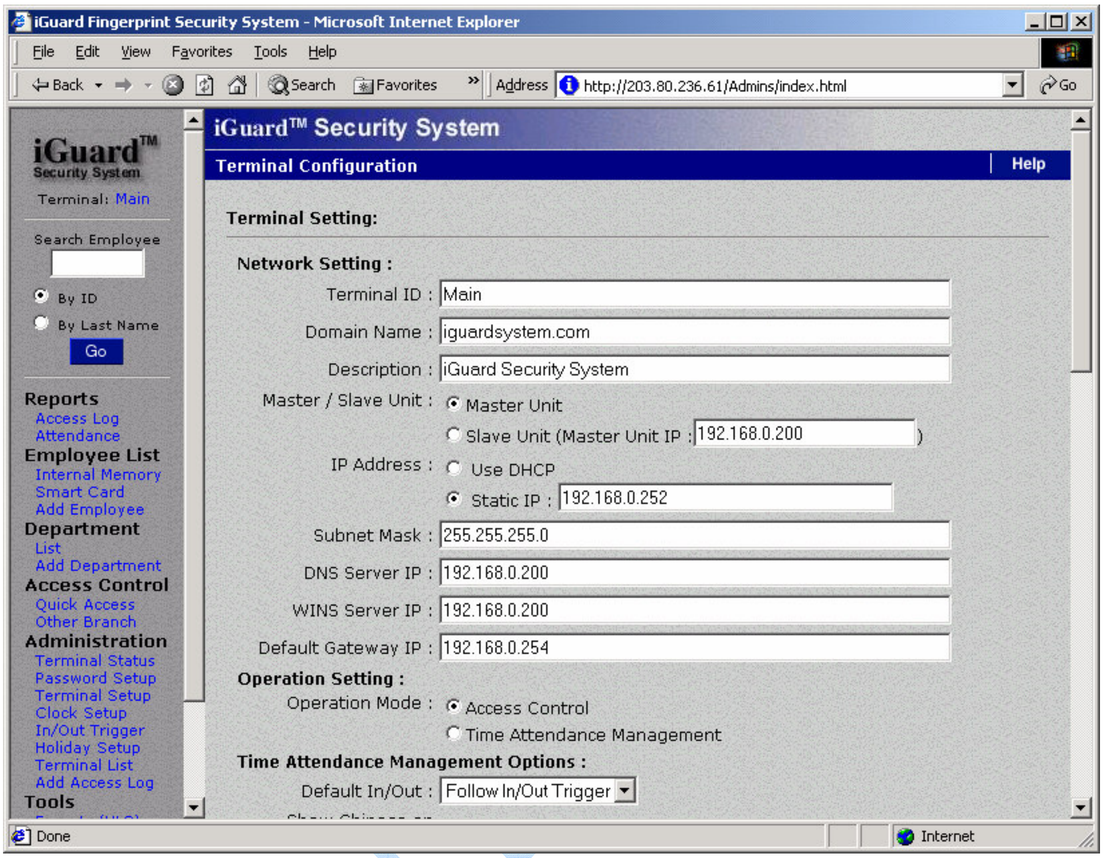
Serial No : VK-9940-0132-F121

Remarks: 1.For security reason, System Administartion User Name and Password cannot leave blank.
2.Leave blank in User Administration User Name will disable User Administration Account.
3.Leave blank in Door Access Password will disable Door Access Password.

Last Updated: Mon, 2 Jul 2001 18:47:18
©2000 Lucky Technology. All rights reserved.

4.9. Administration - Terminal Setup

Select Terminal Setup:



Terminal Configuration

Terminal Setting:

Network Setting :

Terminal ID : Main

Domain Name : iguardsystem.com

Description : iGuard Security System

Master / Slave Unit : ● Master Unit
○ Slave Unit (Master Unit IP : 192.168.0.200)

IP Address : ○ Use DHCP
● Static IP : 192.168.0.252

Subnet Mask : 255.255.255.0

DNS Server IP : 192.168.0.200

WINS Server IP : 192.168.0.200

Default Gateway IP : 192.168.0.254

Operation Setting :

Operation Mode : ● Access Control
○ Time Attendance Management

Time Attendance Management Options :

Default In/Out : Follow In/Out Trigger

4.10. Administration - Clock Setup

Auto Date/Time Value: When enabled, the time of your iGuard is automatically configured as the time on your computer system.

Location (Time Zone): To further specify the time zone of your region, please select the right option from this menu.

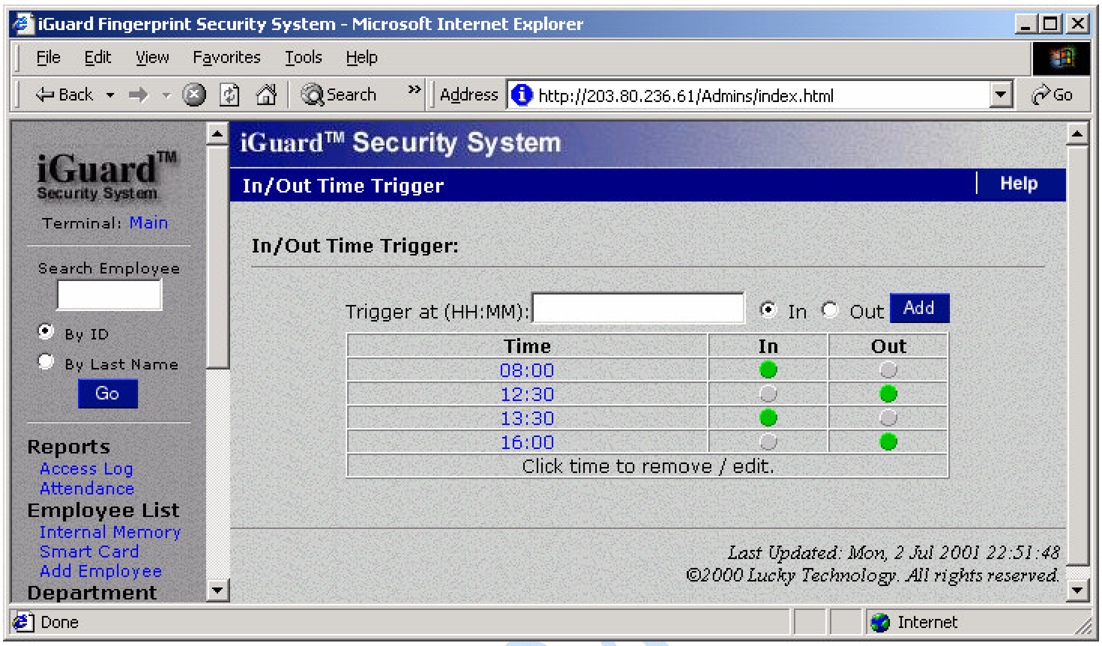
Serial No.: This is the unique serial number of this machine. You may need to provide the information if you need technical support for the device.

There is a software tool to allow you to automatically synchronize the clock with your PC's clock daily. It is available on request basis.

Please also note that if a device is configured as Master device and it has other Slave devices attached in the same network, the new clock setting will automatically update all the slave devices.

4.11. Administration - In / Out Trigger

In / Out time Trigger defines the time for either "IN" or "OUT" for access log.



http://203.80.236.61/Admins/index.html

iGuard™ Security System

In/Out Time Trigger

In/Out Time Trigger:

Trigger at (HH:MM): ◉ In ○ Out Add

Time	In	Out
08:00	●	○
12:30	○	●
13:30	●	○
16:00	○	●

Click time to remove / edit.

Last Updated: Mon, 2 Jul 2001 22:51:48
©2000 Lucky Technology. All rights reserved.

The In / Out Time Setting is useful only if the device is configured for Time Attendance purpose. In the above setting, the device will set the default In / Out as IN at 6:00 am, and will set it to OUT at 12:00pm... etc.

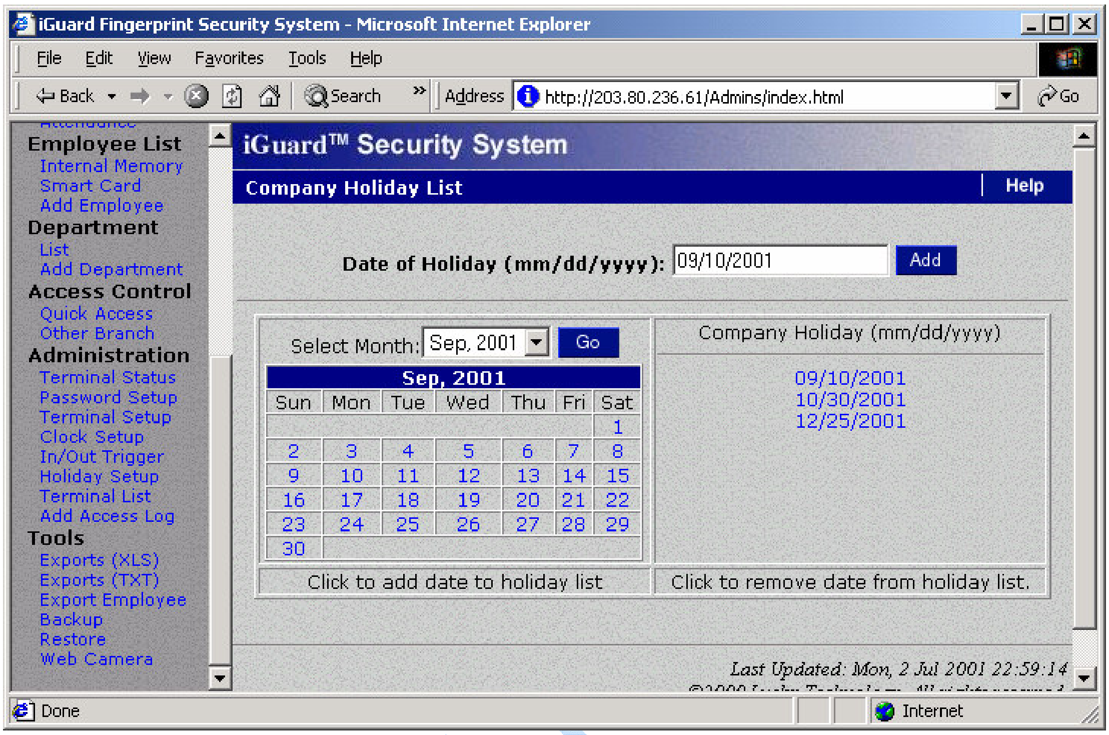
The default In / Out status is shown on the LCD panel of the device as shown:

Description	***LCD Display***
Default IN (stands for Clocking IN).	**Monday 30 13:49** **ID#_ IN**
Default OUT (stands for Clocking OUT).	**Monday 30 13:49** **ID#_ OUT**

User can override the default setting by pressing the backspace key before entering the user ID.

4.12. Administration - Holiday Setup

The Holiday list is used for the Time Restriction purpose (along with the day-of-week settings).



iGuard Fingerprint Security System - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Address Go

http://203.80.236.61/Admins/index.html

Employee List
- Internal Memory
- Smart Card
- Add Employee

Department
- List
- Add Department

Access Control
- Quick Access
- Other Branch

Administration
- Terminal Status
- Password Setup
- Terminal Setup
- Clock Setup
- In/Out Trigger
- Holiday Setup
- Terminal List
- Add Access Log

Tools
- Exports (XLS)
- Exports (TXT)
- Export Employee
- Backup
- Restore
- Web Camera

iGuard™ Security System

Company Holiday List | Help

Date of Holiday (mm/dd/yyyy): 09/10/2001 Add

Select Month: Sep, 2001 Go

Sep, 2001

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						

Click to add date to holiday list

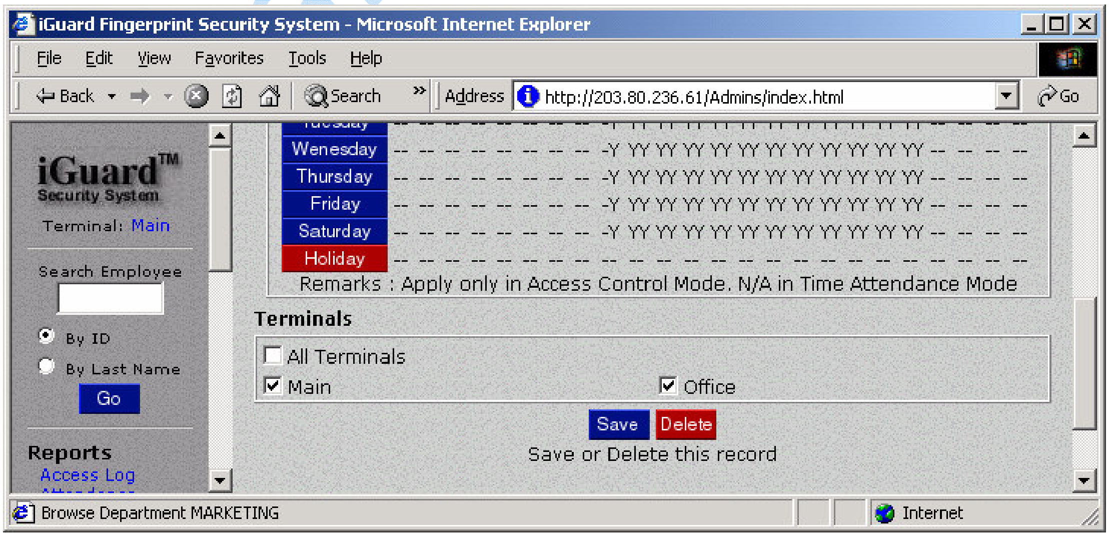
Company Holiday (mm/dd/yyyy)

09/10/2001
10/30/2001
12/25/2001

Click to remove date from holiday list.

Last Updated: Mon, 2 Jul 2001 22:59:14

In the above example, the dates 09/10/2001, 10/30/2001 & 12/25/2001 are set as holidays. On these day, the authorized time will follow the settings for the date "Holiday", as shown in the following: -



iGuard Fingerprint Security System - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Address Go

http://203.80.236.61/Admins/index.html

iGuard™ Security System

Terminal: Main

Search Employee

● By ID
○ By Last Name
Go

Reports
- Access Log

Wenesday	--	--	--	--	--	--	--	--	-Y	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	--	--	--	--
Thursday	--	--	--	--	--	--	--	--	-Y	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	--	--	--	--
Friday	--	--	--	--	--	--	--	--	-Y	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	--	--	--	--
Saturday	--	--	--	--	--	--	--	--	-Y	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	YY	--	--	--	--
Holiday	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Remarks : Apply only in Access Control Mode. N/A in Time Attendance Mode

Terminals

□ All Terminals
☑ Main ☑ Office

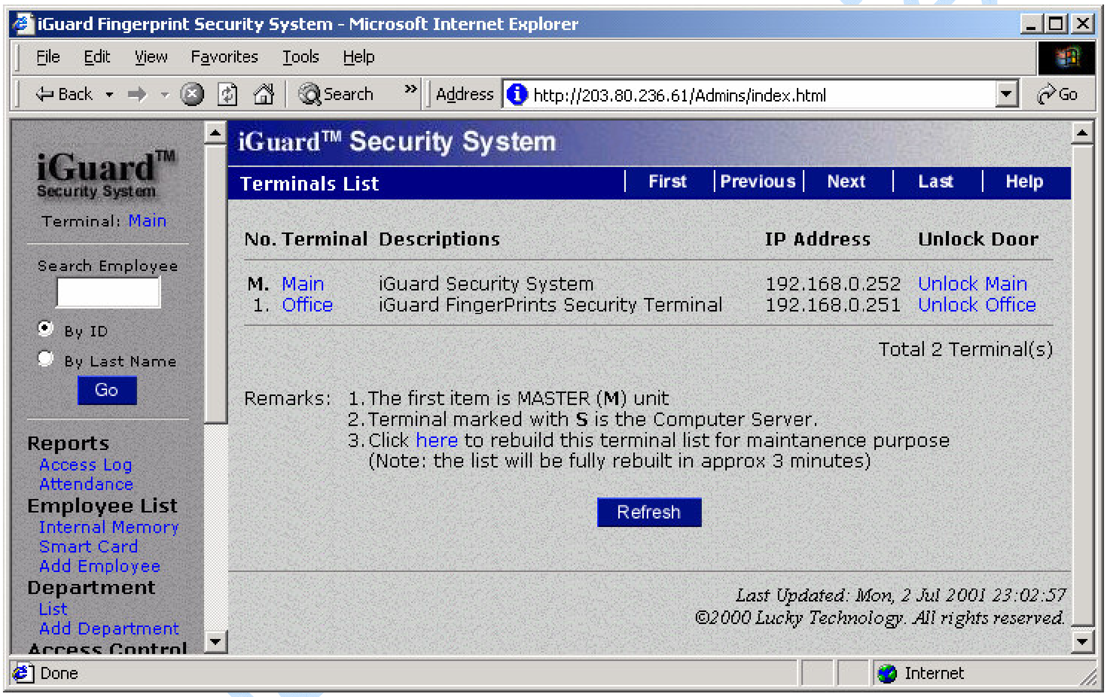
Save Delete
Save or Delete this record

As indicated in the above page, all the employees belong to the Marketing department will not be able to authenticate on the three holidays specified.

Please refer to the section "Department - List" above for how to change the time restriction settings.

4.13. Administration - Terminal List

This page shows the current slave devices in a master and slave mode network.



Terminals List

No.	Terminal	Descriptions	IP Address	Unlock Door
M.	Main	iGuard Security System	192.168.0.252	Unlock Main
1.	Office	iGuard FingerPrints Security Terminal	192.168.0.251	Unlock Office

Total 2 Terminal(s)

Remarks:
1. The first item is MASTER (M) unit
2. Terminal marked with **S** is the Computer Server.
3. Click here to rebuild this terminal list for maintanence purpose (Note: the list will be fully rebuilt in approx 3 minutes)

Refresh

Last Updated: Mon, 2 Jul 2001 23:02:57
©2000 Lucky Technology. All rights reserved.

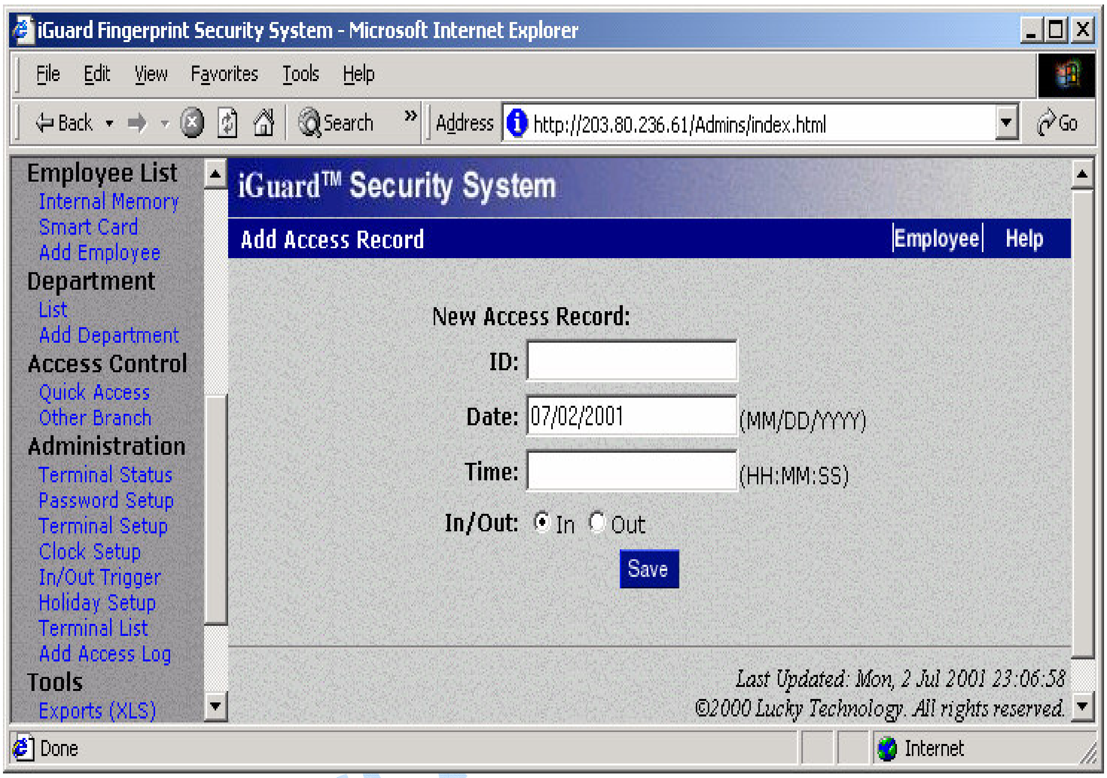
In the above example, the device "Main" is the master unit, and it has one slave unit named "Office".

The corresponding IP address of each device is also shown.

As a convenient feature, you can remotely unlock the doors by clicking the **Unlock Main** & the **Unlock Office**, as well as **Reset Main or Reset Office** links.

4.14. Administration - Add Access Log

By default, all the access records cannot be changed and deleted. However, you can add an access record for an employee should he forgot to Clock-In or Clock-Out. This feature is usually required only for the payroll purpose.



New Access Record:

ID:

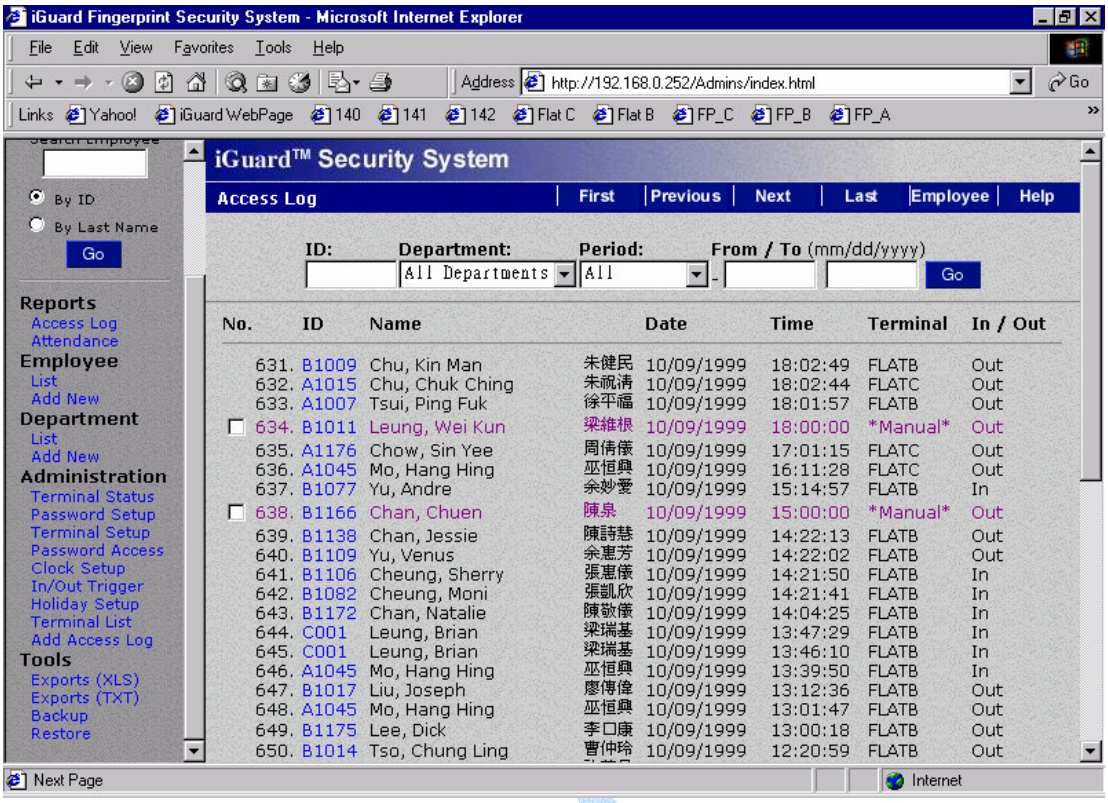
Date: 07/02/2001 (MM/DD/YYYY)

Time: (HH:MM:SS)

In/Out: ● In ○ Out

Last Updated: Mon, 2 Jul 2001 23:06:58
©2000 Lucky Technology. All rights reserved.

A manually added record is shown differently in the access report as shown below: -



ID: Department: All Departments Period: All From / To (mm/dd/yyyy)

No.	ID	Name		Date	Time	Terminal	In / Out
631.	B1009	Chu, Kin Man	朱健民	10/09/1999	18:02:49	FLATB	Out
632.	A1015	Chu, Chuk Ching	朱祝清	10/09/1999	18:02:44	FLATC	Out
633.	A1007	Tsui, Ping Fuk	徐平福	10/09/1999	18:01:57	FLATB	Out
□ 634.	B1011	Leung, Wei Kun	梁維根	10/09/1999	18:00:00	*Manual*	Out
635.	A1176	Chow, Sin Yee	周倩儀	10/09/1999	17:01:15	FLATC	Out
636.	A1045	Mo, Hang Hing	巫恒興	10/09/1999	16:11:28	FLATC	Out
637.	B1077	Yu, Andre	余妙雯	10/09/1999	15:14:57	FLATB	In
□ 638.	B1166	Chan, Chuen	陳泉	10/09/1999	15:00:00	*Manual*	Out
639.	B1138	Chan, Jessie	陳詩慧	10/09/1999	14:22:13	FLATB	Out
640.	B1109	Yu, Venus	余惠芳	10/09/1999	14:22:02	FLATB	Out
641.	B1106	Cheung, Sherry	張惠儀	10/09/1999	14:21:50	FLATB	In
642.	B1082	Cheung, Moni	張凱欣	10/09/1999	14:21:41	FLATB	In
643.	B1172	Chan, Natalie	陳敬儀	10/09/1999	14:04:25	FLATB	In
644.	C001	Leung, Brian	梁瑞基	10/09/1999	13:47:29	FLATB	In
645.	C001	Leung, Brian	梁瑞基	10/09/1999	13:46:10	FLATB	In
646.	A1045	Mo, Hang Hing	巫恒興	10/09/1999	13:39:50	FLATB	In
647.	B1017	Liu, Joseph	廖傳偉	10/09/1999	13:12:36	FLATB	Out
648.	A1045	Mo, Hang Hing	巫恒興	10/09/1999	13:01:47	FLATB	Out
649.	B1175	Lee, Dick	李口康	10/09/1999	13:00:18	FLATB	Out
650.	B1014	Tso, Chung Ling	曹仲玲	10/09/1999	12:20:59	FLATB	Out

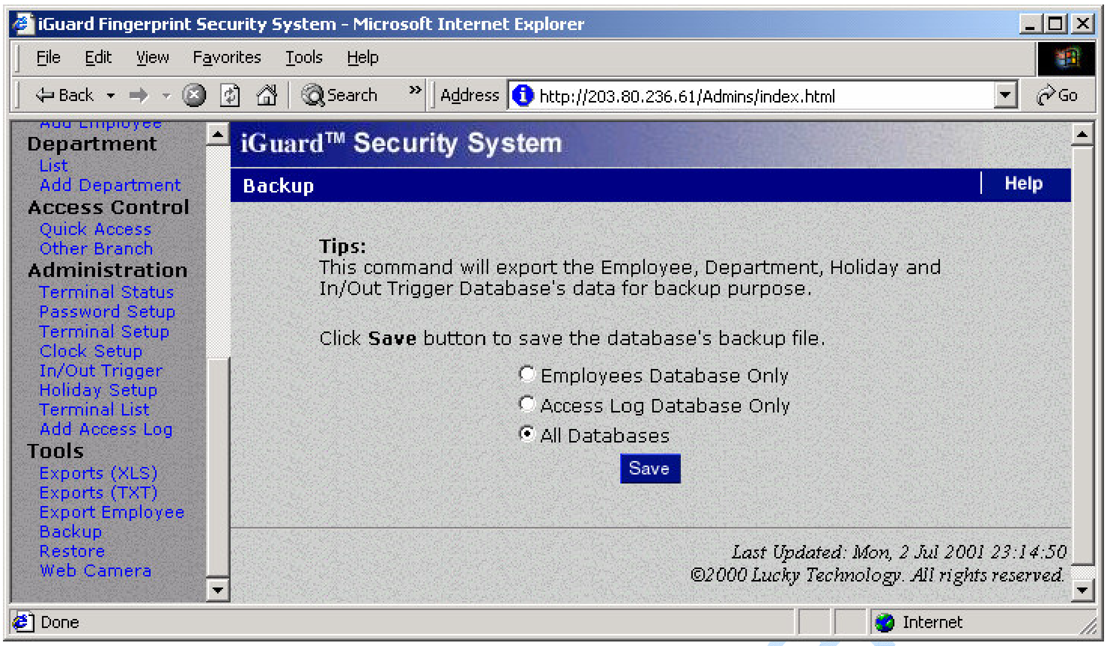
The records in pink color with the checkbox next to them indicate that these records were added manually. You can later on delete these records by selecting the checkbox and then press the **Delete** button at the bottom of the page.

4.15. Tools - Export Employee

Select Export Employee to export a particular or group of Employees by ID.

4.16. Tools - Backup & Restore

It is suggested to backup the internal data periodically to the desktop computer (such as a daily backup). In the unlikely event that the system is to be replaced, the old data can be restored back to the new device, and the employees do not need to re-enroll again.



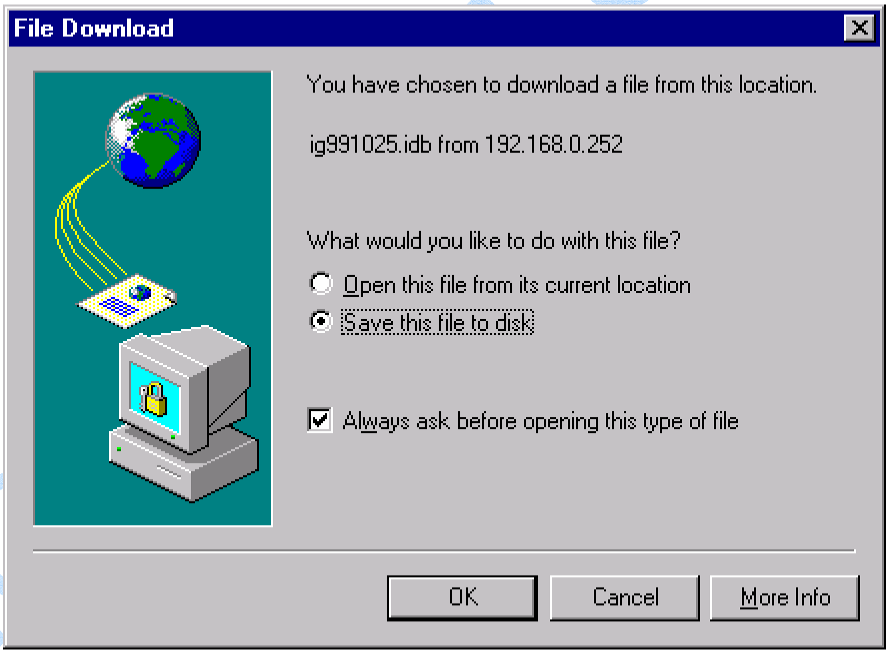
Tips:
This command will export the Employee, Department, Holiday and In/Out Trigger Database's data for backup purpose.

Click **Save** button to save the database's backup file.

○ Employees Database Only
○ Access Log Database Only
● All Databases

Last Updated: Mon, 2 Jul 2001 23:14:50
©2000 Lucky Technology. All rights reserved.

Press the **Save** button, and a dialog box similar to the one below should appear: -



You have chosen to download a file from this location.

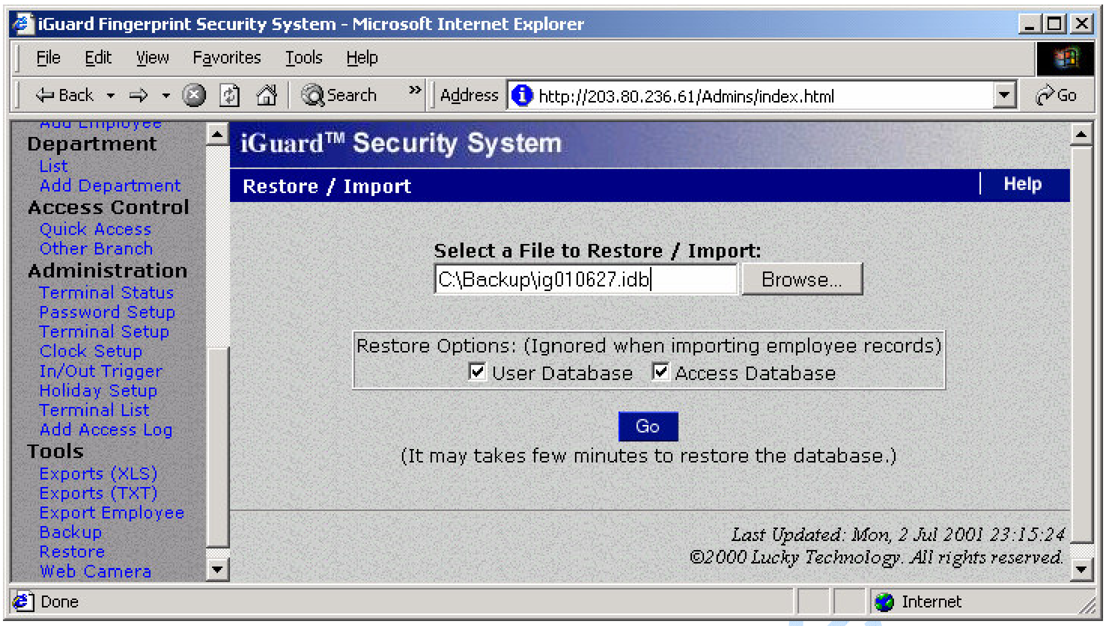
ig991025.idb from 192.168.0.252

What would you like to do with this file?
○ Open this file from its current location
● Save this file to disk

☑ Always ask before opening this type of file

Press the **OK** button to save the backup data to your desktop computer.

When it is necessary to restore the data (for example, a new device has been installed), go to the Restore page and specify the file name as follows: -



Select a File to Restore / Import: C:\Backup\ig010627.idb

Restore Options: (Ignored when importing employee records)
☑ User Database ☑ Access Database

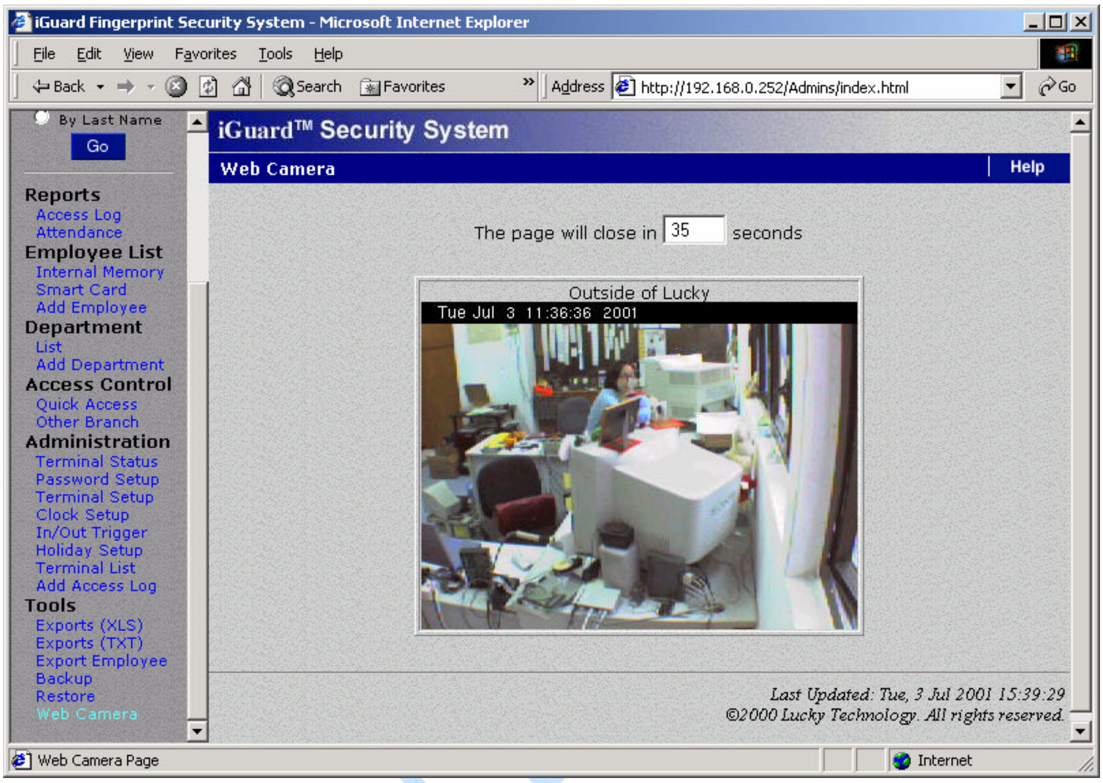
(It may takes few minutes to restore the database.)

Last Updated: Mon, 2 Jul 2001 23:15:24
©2000 Lucky Technology. All rights reserved.

Press the **Go** button and the data will be restored from the file to the device.

4.17. Tools - Web Camera

If the optional Web Camera is available to the network, iGuard can redirect the web camera's image to the browser as shown below: -



The page will close in 35 seconds

Last Updated: Tue, 3 Jul 2001 15:39:29
©2000 Lucky Technology. All rights reserved.

Currently the only supported web camera is *Axis 2100 Network Camera* from *Axis Communications* and the *JVC camera* from *JVC.*[1] Up to four Web Cameras can be supported at the same time and shown in the same page.

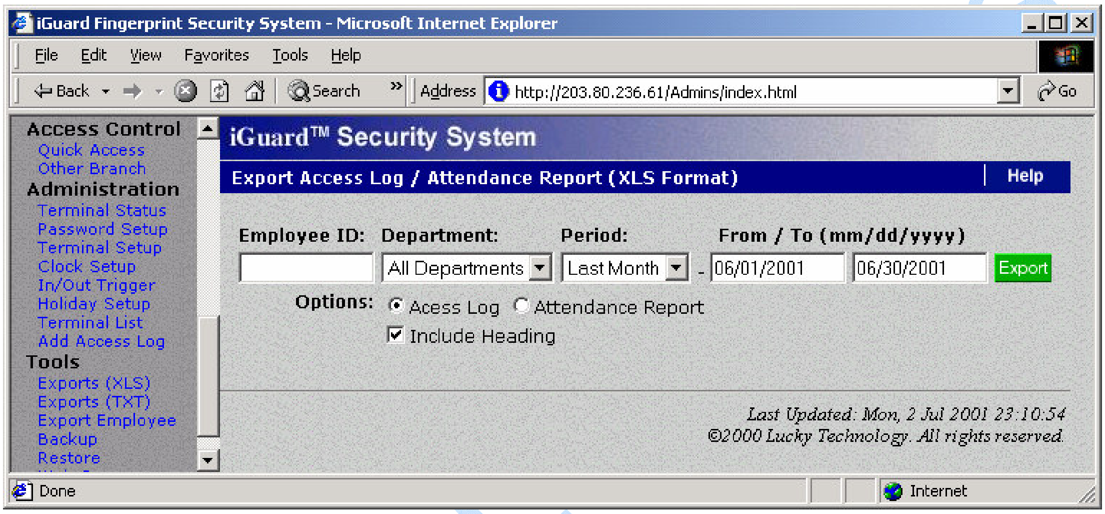
Please refer to the Administration - Terminal Setup section for more details in setting up the web cameras.

http://www.axis.com

5 REPORTING

5.1. Tools-Export (XLS)

The reports (including the Access Report & Attendance Report) can be exported directly in the popular XLS format, which enables smooth integration with office suite applications such as Microsoft EXCEL. Various reports can then be easily generated using the built-in features of the office suite application. In this way, companies can design their own report formats that are best suitable to their existing operations.



Export Access Log / Attendance Report (XLS Format)

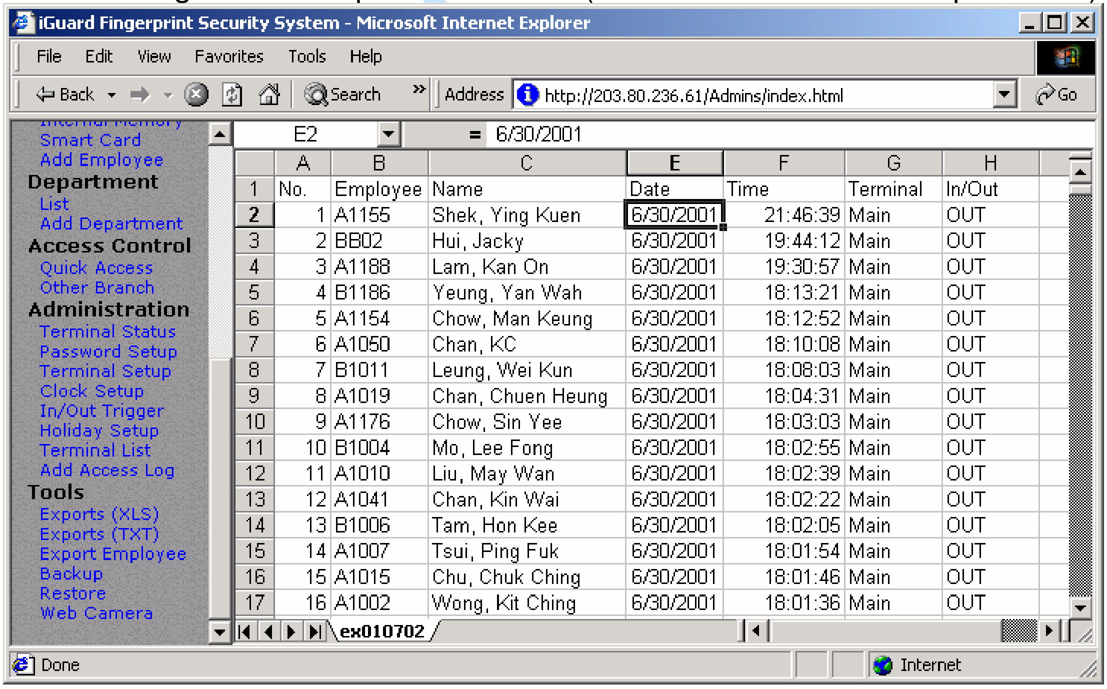
Employee ID: Department: All Departments Period: Last Month From / To (mm/dd/yyyy) 06/01/2001 - 06/30/2001

Options: ● Acess Log ○ Attendance Report

☑ Include Heading

Last Updated: Mon, 2 Jul 2001 23:10:54
©2000 Lucky Technology. All rights reserved.

The following is an example of the result (with Microsoft Internet Explorer 5.0): -



E2 = 6/30/2001

	A	B	C	E	F	G	H
1	No.	Employee	Name	Date	Time	Terminal	In/Out
2	1	A1155	Shek, Ying Kuen	6/30/2001	21:46:39	Main	OUT
3	2	BB02	Hui, Jacky	6/30/2001	19:44:12	Main	OUT
4	3	A1188	Lam, Kan On	6/30/2001	19:30:57	Main	OUT
5	4	B1186	Yeung, Yan Wah	6/30/2001	18:13:21	Main	OUT
6	5	A1154	Chow, Man Keung	6/30/2001	18:12:52	Main	OUT
7	6	A1050	Chan, KC	6/30/2001	18:10:08	Main	OUT
8	7	B1011	Leung, Wei Kun	6/30/2001	18:08:03	Main	OUT
9	8	A1019	Chan, Chuen Heung	6/30/2001	18:04:31	Main	OUT
10	9	A1176	Chow, Sin Yee	6/30/2001	18:03:03	Main	OUT
11	10	B1004	Mo, Lee Fong	6/30/2001	18:02:55	Main	OUT
12	11	A1010	Liu, May Wan	6/30/2001	18:02:39	Main	OUT
13	12	A1041	Chan, Kin Wai	6/30/2001	18:02:22	Main	OUT
14	13	B1006	Tam, Hon Kee	6/30/2001	18:02:05	Main	OUT
15	14	A1007	Tsui, Ping Fuk	6/30/2001	18:01:54	Main	OUT
16	15	A1015	Chu, Chuk Ching	6/30/2001	18:01:46	Main	OUT
17	16	A1002	Wong, Kit Ching	6/30/2001	18:01:36	Main	OUT

5.2. Tools - Exports (TXT)

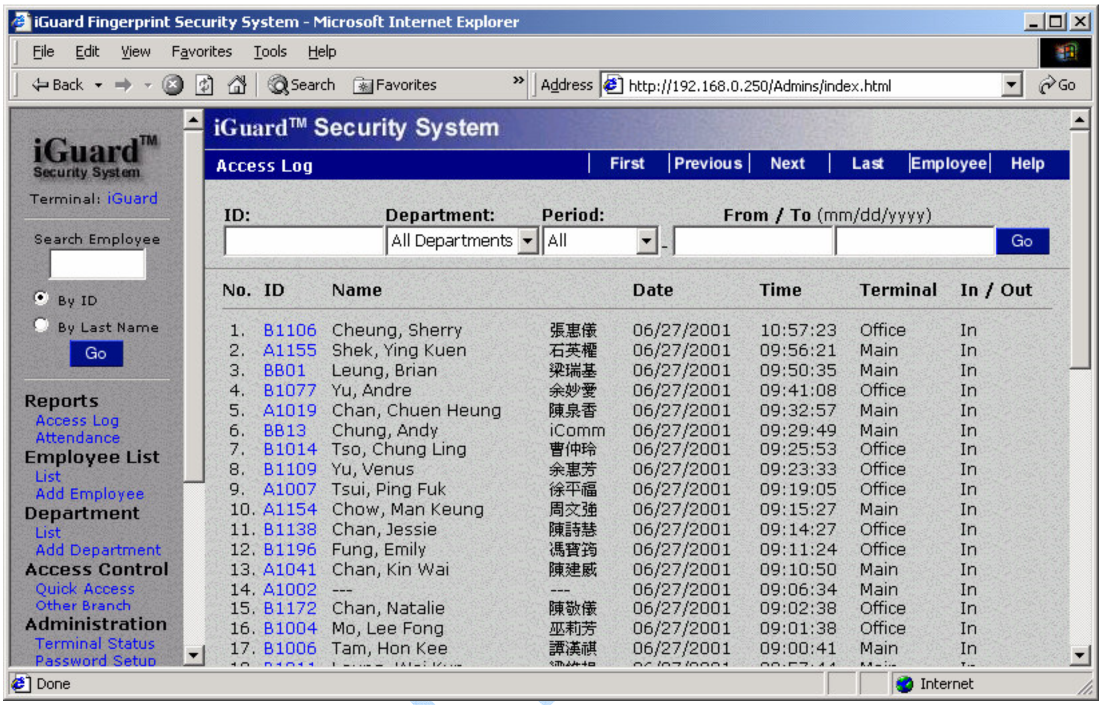
The TEXT file is useful for exporting to existing payroll programs used in the company.

The format of the text file is as follows:

```
"Item","Employee ID","Name","Other Name","Date","Time","Terminal","In/Out"

"1","A1155","Shek, Ying Kuen","admin","09/30/1999","20:02:04","F1103","Out"

"2","B1077","Yu, Andre","account","09/30/1999","19:58:58","FLATB","Out"

"3","C001","Leung, Brian","director","09/30/1999","19:58:50","FLATB","Out"

"4","B1166","Chan, Chuen","support","09/30/1999","19:56:45","FLATB","Out"

"5","A1174","Go, Kai Yin","engineer","09/30/1999","19:52:30","F1103","In"

"6","B1082","Cheung, Moni","engineer","09/30/1999","19:21:05","FLATB","Out"

"7","B1011","Leung, Wei Kun","manager","09/30/1999","19:06:18","FLATB","Out"

"8","B1067","Lau, Ester","engineer","09/30/1999","18:58:11","FLATB","Out"

"9","A1154","Chow, Man Keung","assistant","09/30/1999","18:36:48","F1103","Out"

"10","A1050","Chan, KC","support","09/30/1999","18:20:59","FLATB","Out"

"11","A1002","Wong, Kit Ching","shipping","09/30/1999","18:19:07","F1103","Out"
```

5.3. Reports - Access Log

Click on the link **Access Log** in the left panel, and you should see something similar to the following screen: -



ID:
Department: All Departments
Period: All
From / To (mm/dd/yyyy)
Go

No.	ID	Name		Date	Time	Terminal	In / Out
1.	B1106	Cheung, Sherry	張惠儀	06/27/2001	10:57:23	Office	In
2.	A1155	Shek, Ying Kuen	石英權	06/27/2001	09:56:21	Main	In
3.	BB01	Leung, Brian	梁瑞基	06/27/2001	09:50:35	Main	In
4.	B1077	Yu, Andre	余妙愛	06/27/2001	09:41:08	Office	In
5.	A1019	Chan, Chuen Heung	陳泉香	06/27/2001	09:32:57	Main	In
6.	BB13	Chung, Andy	iComm	06/27/2001	09:29:49	Main	In
7.	B1014	Tso, Chung Ling	曹仲玲	06/27/2001	09:25:53	Office	In
8.	B1109	Yu, Venus	余惠芳	06/27/2001	09:23:33	Office	In
9.	A1007	Tsui, Ping Fuk	徐平福	06/27/2001	09:19:05	Office	In
10.	A1154	Chow, Man Keung	周文強	06/27/2001	09:15:27	Main	In
11.	B1138	Chan, Jessie	陳詩慧	06/27/2001	09:14:27	Office	In
12.	B1196	Fung, Emily	馮寶筠	06/27/2001	09:11:24	Office	In
13.	A1041	Chan, Kin Wai	陳建威	06/27/2001	09:10:50	Main	In
14.	A1002	---	---	06/27/2001	09:06:34	Main	In
15.	B1172	Chan, Natalie	陳敬儀	06/27/2001	09:02:38	Office	In
16.	B1004	Mo, Lee Fong	巫莉芳	06/27/2001	09:01:38	Office	In
17.	B1006	Tam, Hon Kee	譚漢祺	06/27/2001	09:00:41	Main	In

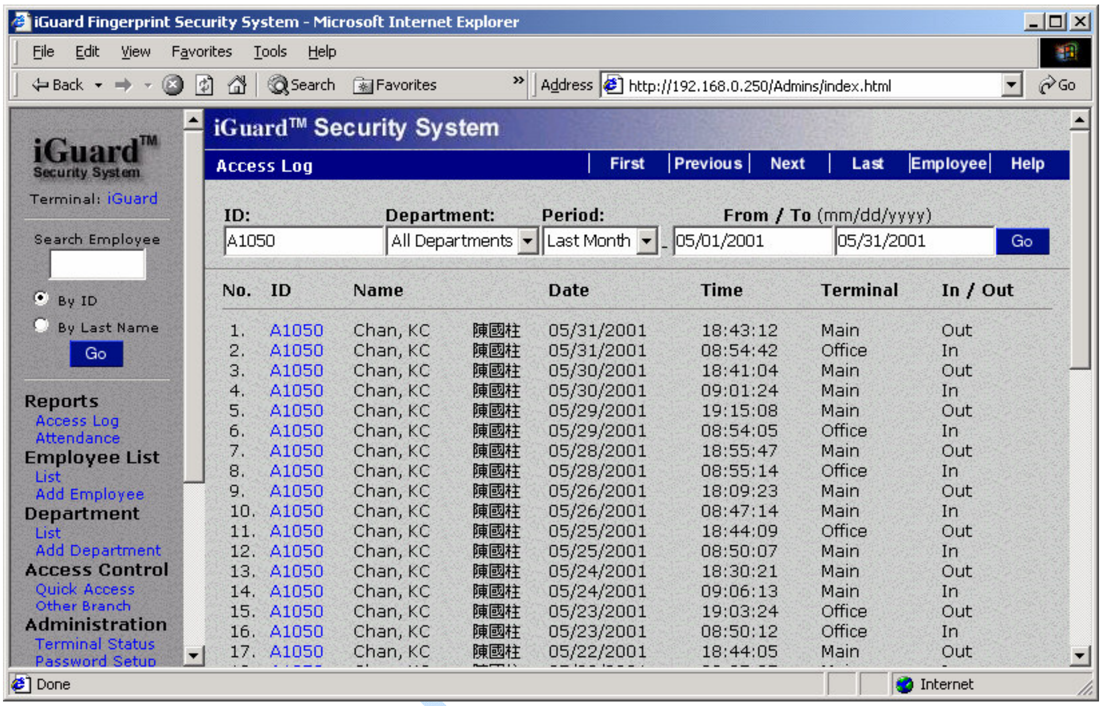
This page shows the employees' Access Records. If you want to show the records of only a particular person (e.g., C001), enter his/her ID # in the edit box and press the **Go** button, and the browser will only show the records of this person.

You can also specify the Department, and only the particular department members will be shown.

The *Time Period* can also be limited, which would display only records specified. You can also specify the Time Period by choosing the *Range* selection and entering directly to the From / To fields.

To browse the records, such as to move to next page, press the **Next** button in the navigator bar at the top of the page, or jump to any particular page by clicking on the page number at the bottom.

The following example shows only the previous month records of the employee ID # BB26:

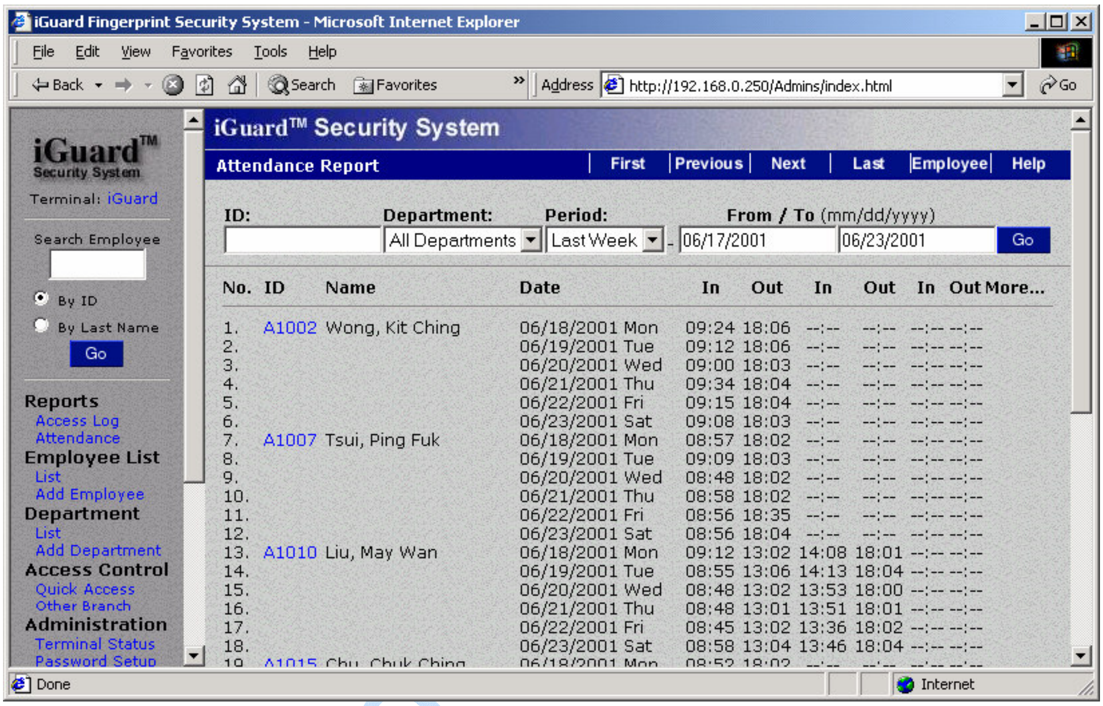


ID: A1050
Department: All Departments
Period: Last Month
From / To (mm/dd/yyyy) 05/01/2001 – 05/31/2001

No.	ID	Name		Date	Time	Terminal	In / Out
1.	A1050	Chan, KC	陳國柱	05/31/2001	18:43:12	Main	Out
2.	A1050	Chan, KC	陳國柱	05/31/2001	08:54:42	Office	In
3.	A1050	Chan, KC	陳國柱	05/30/2001	18:41:04	Main	Out
4.	A1050	Chan, KC	陳國柱	05/30/2001	09:01:24	Main	In
5.	A1050	Chan, KC	陳國柱	05/29/2001	19:15:08	Main	Out
6.	A1050	Chan, KC	陳國柱	05/29/2001	08:54:05	Office	In
7.	A1050	Chan, KC	陳國柱	05/28/2001	18:55:47	Main	Out
8.	A1050	Chan, KC	陳國柱	05/28/2001	08:55:14	Office	In
9.	A1050	Chan, KC	陳國柱	05/26/2001	18:09:23	Main	Out
10.	A1050	Chan, KC	陳國柱	05/26/2001	08:47:14	Main	In
11.	A1050	Chan, KC	陳國柱	05/25/2001	18:44:09	Office	Out
12.	A1050	Chan, KC	陳國柱	05/25/2001	08:50:07	Main	In
13.	A1050	Chan, KC	陳國柱	05/24/2001	18:30:21	Main	Out
14.	A1050	Chan, KC	陳國柱	05/24/2001	09:06:13	Main	In
15.	A1050	Chan, KC	陳國柱	05/23/2001	19:03:24	Office	Out
16.	A1050	Chan, KC	陳國柱	05/23/2001	08:50:12	Office	In
17.	A1050	Chan, KC	陳國柱	05/22/2001	18:44:05	Main	Out

5.4. Reports - Attendance

The attendance reports provide consolidated access records as follows: -



iGuard™ Security System

Attendance Report | First | Previous | Next | Last | Employee | Help

ID:
Department: All Departments
Period: Last Week
From / To (mm/dd/yyyy) 06/17/2001 - 06/23/2001
Go

No.	ID	Name	Date	In	Out	In	Out	In	Out	More...
1.	A1002	Wong, Kit Ching	06/18/2001 Mon	09:24	18:06	--:--	--:--	--:--	--:--	
2.			06/19/2001 Tue	09:12	18:06	--:--	--:--	--:--	--:--	
3.			06/20/2001 Wed	09:00	18:03	--:--	--:--	--:--	--:--	
4.			06/21/2001 Thu	09:34	18:04	--:--	--:--	--:--	--:--	
5.			06/22/2001 Fri	09:15	18:04	--:--	--:--	--:--	--:--	
6.			06/23/2001 Sat	09:08	18:03	--:--	--:--	--:--	--:--	
7.	A1007	Tsui, Ping Fuk	06/18/2001 Mon	08:57	18:02	--:--	--:--	--:--	--:--	
8.			06/19/2001 Tue	09:09	18:03	--:--	--:--	--:--	--:--	
9.			06/20/2001 Wed	08:48	18:02	--:--	--:--	--:--	--:--	
10.			06/21/2001 Thu	08:58	18:02	--:--	--:--	--:--	--:--	
11.			06/22/2001 Fri	08:56	18:35	--:--	--:--	--:--	--:--	
12.			06/23/2001 Sat	08:56	18:04	--:--	--:--	--:--	--:--	
13.	A1010	Liu, May Wan	06/18/2001 Mon	09:12	13:02	14:08	18:01	--:--	--:--	
14.			06/19/2001 Tue	08:55	13:06	14:13	18:04	--:--	--:--	
15.			06/20/2001 Wed	08:48	13:02	13:53	18:00	--:--	--:--	
16.			06/21/2001 Thu	08:48	13:01	13:51	18:01	--:--	--:--	
17.			06/22/2001 Fri	08:45	13:02	13:36	18:02	--:--	--:--	
18.			06/23/2001 Sat	08:58	13:04	13:46	18:04	--:--	--:--	
19.	A1015	Chu, Chuk Ching	06/18/2001 Mon	08:52	18:02	--:--	--:--	--:--	--:--	

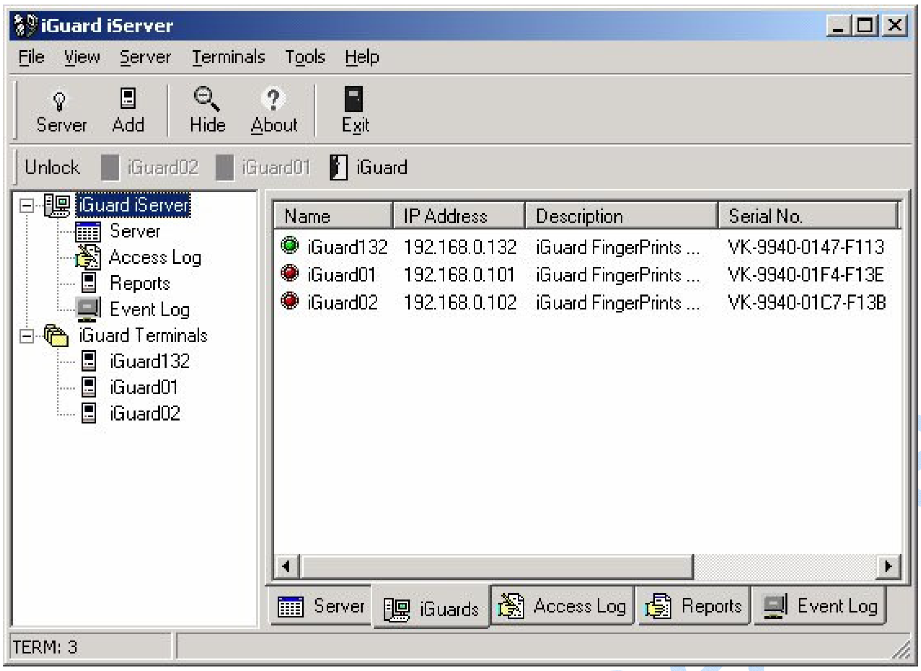
***Daily In/Out

The Attendance Report is particularly useful for payroll purpose. Similar to the Access Log Report, you can specify the employee's ID and / or the Time Period of the Attendance Report.

5.5. iServer

iServer is Windows based program to collect transaction records from iGuards and to save them on ODBC database format. iServer is default using Microsoft Access.

If you want to use other ODBC compliance database other than MS Access, you have to do the following things in order to get the iServer connect to the database. The syntax is subject to the database you have.


iGuard iServer
File View Server Terminals Tools Help
Server Add Hide About Exit
Unlock iGuard02 iGuard01 iGuard
iGuard iServer
Server
Access Log
Reports
Event Log
iGuard Terminals
iGuard132
iGuard01
iGuard02
Server iGuards Access Log Reports Event Log
TERM: 3

Name	IP Address	Description	Serial No.
iGuard132	192.168.0.132	iGuard FingerPrints ...	VK-9940-0147-F113
iGuard01	192.168.0.101	iGuard FingerPrints ...	VK-9940-01F4-F13E
iGuard02	192.168.0.102	iGuard FingerPrints ...	VK-9940-01C7-F13B

Creating Database

You need to create a database, and create 2 tables. We have examples from 2 kinds of databases.

The Table Structure of the Default MS Access (ibonussrv.mdb):

5.5.1. MS Access

Table: AccessLog

RCDID Int AUTO_INCREMENT,

EmployeeID char(16),

LogDate char(10),

LogTime char(10),

TerminalID char(20),

InOut Int,

Primary Key(RCDID, EmployeeID, LogDate, LogTime, TerminalID)

Table: Employee

EmployeeID char(16),

LastName char(40),

FirstName char(40),

OtherName char(40),

Password char(16),

EmpStatus Int,

NumMinutiae1 Int,

NumMinutiae2 Int,

PhotoFile char(40),

Minutiae1 image,

Minutiae2 image,

Photo image,

Department char(50),

Primary Key(EmployeeID)

There are some differences in the syntax of creating the table in other database like SQL Sever and Oracle. The following is for you reference.

5.5.2. SQL Server

Table: AccessLog

RCDID Int IDENTITY yes,

EmployeeID char(16),

LogDate char(10),

LogTime char(10),

TerminalID char(20),

InOut Int,

Primary Key(RCDID, EmployeeID, LogDate, LogTime, TerminalID)

Table: Employee

The same syntax as MS Access

The database created in SQL Server need to have a login in order to access the tables. Can do it in the step of creating the DSN later.

5.5.3. Oracle

Table: AccessLog

RCDID Number(38) Not Null, <- Contraint – Auto Increment field

EmployeeID Char(16) Not Null,

LogDate Char(10) Not Null,

LogTime Char(10) Not Null,

TerminalID Char(20) Not Null,

InOut Number(38)

Table: Employee

EmployeeID Char(16) Not Null,

LastName Char(40),

FirstName Char(40),

OtherName Char(40),

Password Char(40),

EmpStatus Number(38),

NumMinutiae1 Number(38),

NumMinutiae2 Number(38),

PhotoFile Char(40),

Minutiae1 BLOB,

Minutiae2 BLOB,

Photo BLOB,

Department Varchar2(50)

It has many method to create a table in Oracle and to do the auto increment field (RCDID). The following method are the most common.

1. To create an Oracle table :
   a) you can use an administration tools in Oracle for table manipulation if you use version which is 8 or later, or ;
   b) you can use sql command to create table in sql plus or sql worksheet.
2. To create a field for auto increment (RCDID):
   a) To create a sequence and add a constriant to a field, or ;
   b) Create a trigger to increment the field.

The same as SQL Server, you need to have a login for the database. You must make sure the username and password is correct and the username should have right access the AccessLog and Employee. You must aware that users in Oracle have their own right to access table. If you do not have username and password, you could not enter into the Oracle database. If your username does not have any right to access the table, you could not do anything to that table even you could log in to the Oracle database. After you have the login for the database, you can test it as the following.

Testing (Optional):

1) Use SQL Plus to login as the same username and password as in iServer.
2) Try select and insert statement to that table in SQL Plus.

5.5.4. Create Data Source Name (DSN)

In Control Panels -> Administrative tools -> ODBC -> System DSN -> Add

For SQL Server and Oracle database, the procedure is similar.

Please specified the Data Source Name to default “iServer”.

For SQL Server database, you can use the login username, say “sa” which has a greatest privilege, and password to create the DSN.

For Oracle , you can try to choose driver “Orahome” if you have and this is the way from our customer success.

Finally, this is worked fine when you start iServer. When you are using the ODBC compatible database other than MS Access, do not choose to create MS Access when it prompted you for the first run.

6 MASTER-SLAVE/SUPER MASTER

6.1 Master vs. Slave Mode

In a multi-device environment where more than one iGuard device are connected to the same corporate network, one device is assigned as the Master device, and all others are assigned as the Slave devices.

Before a person can be identified, the person must submit his/her fingerprint sample to the system, better known as fingerprint enrollment. This can be done in any device, Master or Slave device. The user's data will then be automatically replicated to all other devices. In other words, once you enrolled in the Master device, your fingerprint information is also available in all other slave devices (and vice verse), and you can access any of these devices, as long as you have the appropriate access levels.

All the access records and the Clock-In Clock-Out records are also automatically replicated from the Slave devices to the Master device, and so the Master device contains all the necessary information. Therefore, you only need to do is to access the Master device, using any standard web browser, to obtain all the access and attendance records of the whole system without having to access the Slave devices.

iGuard can be configured to Master or Slave mode. Master and Slave iGuard can be logically connected using TCP/IP protocol. With a RJ45 cable plugged from your iGuard unit to your corporate LAN, you can connect your iGuard to the corporate network. Once you have connected them, you need to configure the units' IP address for functioning, if it is a slave unit, you have to specify its master unit so it can relay all the information to and from the master device.

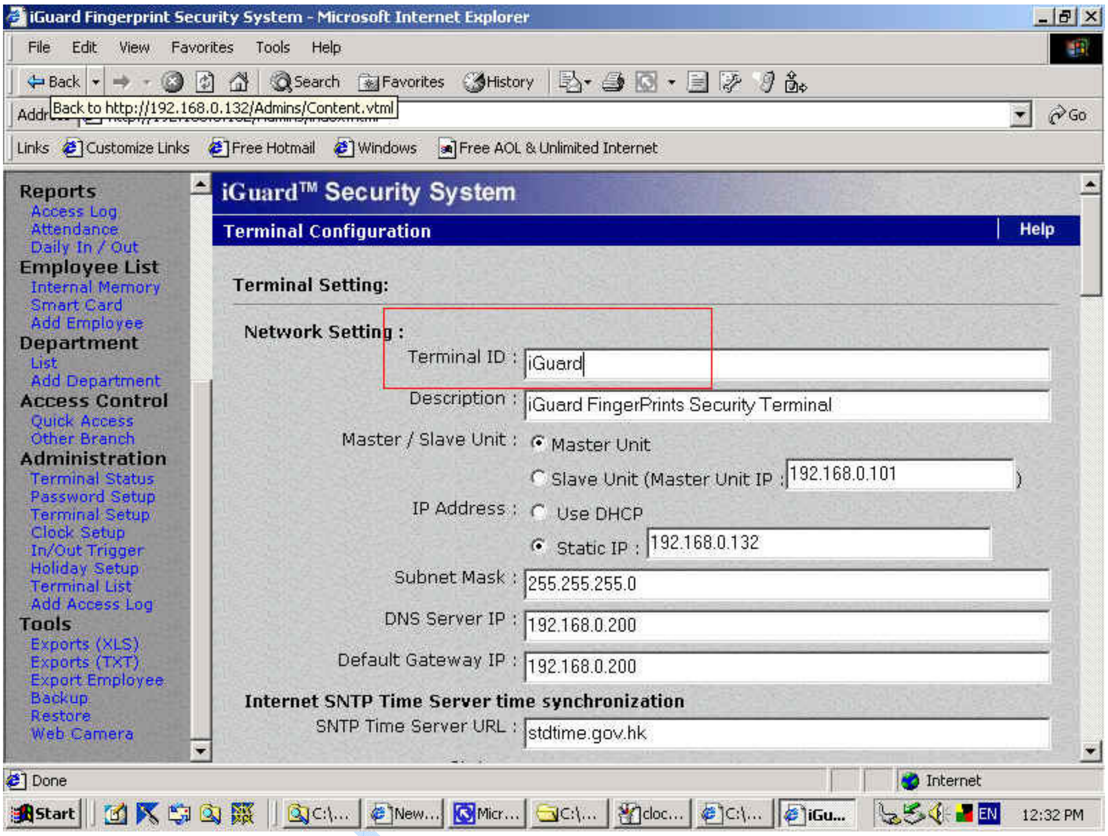
When you add yourself on to a master unit, the unit gives you access to itself and not the other departments due to security reasons. To configure that, you need to go on the web server through the website and click on "List" under Departments. You can click on the default "Everyone". Here, under "Terminals" you need to give yourself access rights to "All Terminals" and click Save.

To synchronize the data between your devices, you MUST set them as Master and Slave Mode. Below, we have depicted on how this can be achieved for an organization with 3-4 devices interconnected in such a configuration.

Warning: LM series and FPS110 series (old) cannot be mixed in the master-slave mode.

6.2 Setting Terminal ID

The terminal ID of each iGuard should be renamed (default: iGuard) to different names so as to avoid confusion in master and slave modes. Select terminal setup in Internet browser and rename the terminal ID accordingly.



Terminal Configuration

Terminal Setting:

Network Setting :

Terminal ID : iGuard

Description : iGuard FingerPrints Security Terminal

Master / Slave Unit : ● Master Unit

○ Slave Unit (Master Unit IP : 192.168.0.101)

IP Address : ○ Use DHCP

● Static IP : 192.168.0.132

Subnet Mask : 255.255.255.0

DNS Server IP : 192.168.0.200

Default Gateway IP : 192.168.0.200

Internet SNTP Time Server time synchronization

SNTP Time Server URL : stdtime.gov.hk

6.3 Super Master

Super Master, a different hardware, is used in the case of more than a thousand users are required in a master-slave mode network.

The Super Master will be used as a master device replacing a standard iGuard master device in the network. With the Super Master, the slave iGuards will operate in cache mode which means that they only store the most recently used 1,000 users in memory. During authentication, if the user can not be found on the slave iGuard, the slave iGuard will request the transfer the user information from the Super Master via network. The new user information will be stored on the slave iGuard and replace the oldest user information. Please also note that users with automatch enabled will always be stored in the cache memory.

Super Master liked iGuard embeddeds web server for remote administration.

7 MISCELLANEOUS

7.1 Remote Door Relay

Remote Door Relay is used for absolute security for access control. In this case, the relay at the back of the iGuard is not used and the Remote Door Relay is installed inside the building.

Remote Door Relay Connection Terminal Description:

ID

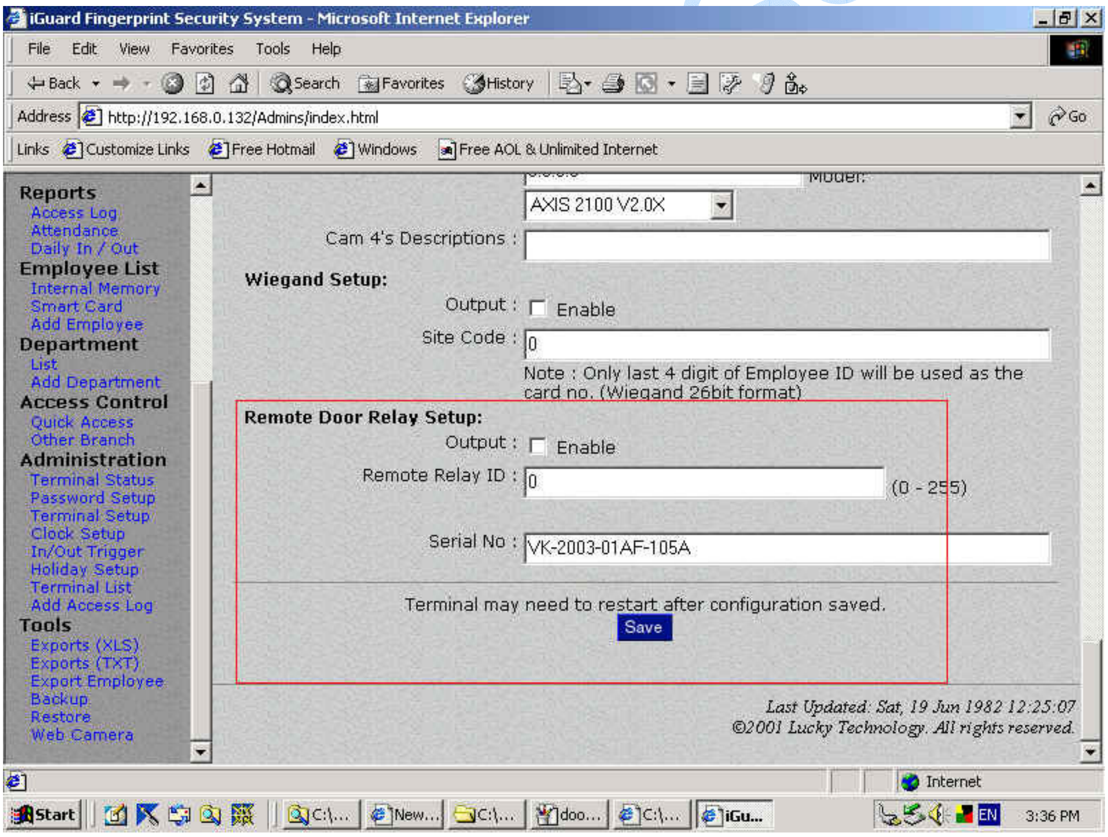
NO	Door Relay's Normal Open
COM	Door Relay's Common
NC	Door Relay's Normal Close
DOOR SW	Door Switch
DOOR SW	Door Switch
A- RS485 Connection	connect to iGuard
B- RS485 Connection	connect to iGuard
+12VDC	+12VDC
GND	GND

Selection Switches:

Turn eight ID selection switches on or off to select the ID number. for the Remote Relay. Each Switch represents a number and the selected ID is the sum of that number. For example, to set the ID of the relay box to 12, turn on switches No. 3 & 4. The following table shows the number of each switch:

Switch	Number	Requirement:
1 2 3 4 5 6 7 8	1 2 4 8 16 32 64 128	In order to use this Remote Door Relay Board, special requirement of iGuard is necessary. 1. Firmware Version: 3.2.9987A or up (can be updated by firmware update patch), 2. iGuard Remote Door Relay hardware support. It can be verified by checking iGuard's status web page; "Remote Door Relay" will be shown in row "Other Feature". If item 2 is not satisfied, you should contact Lucky Technology to obtain a hardware upgrade.

In terminal setup, it has to be enabled.



Model: AXIS 2100 V2.0X

Cam 4's Descriptions :

Wiegand Setup:

Output : □ Enable

Site Code : 0

Note : Only last 4 digit of Employee ID will be used as the card no. (Wiegand 26bit format)

Remote Door Relay Setup:

Output : □ Enable

Remote Relay ID : 0 (0 - 255)

Serial No : VK-2003-01AF-105A

Terminal may need to restart after configuration saved.

Save

Last Updated: Sat, 19 Jun 1982 12:25:07

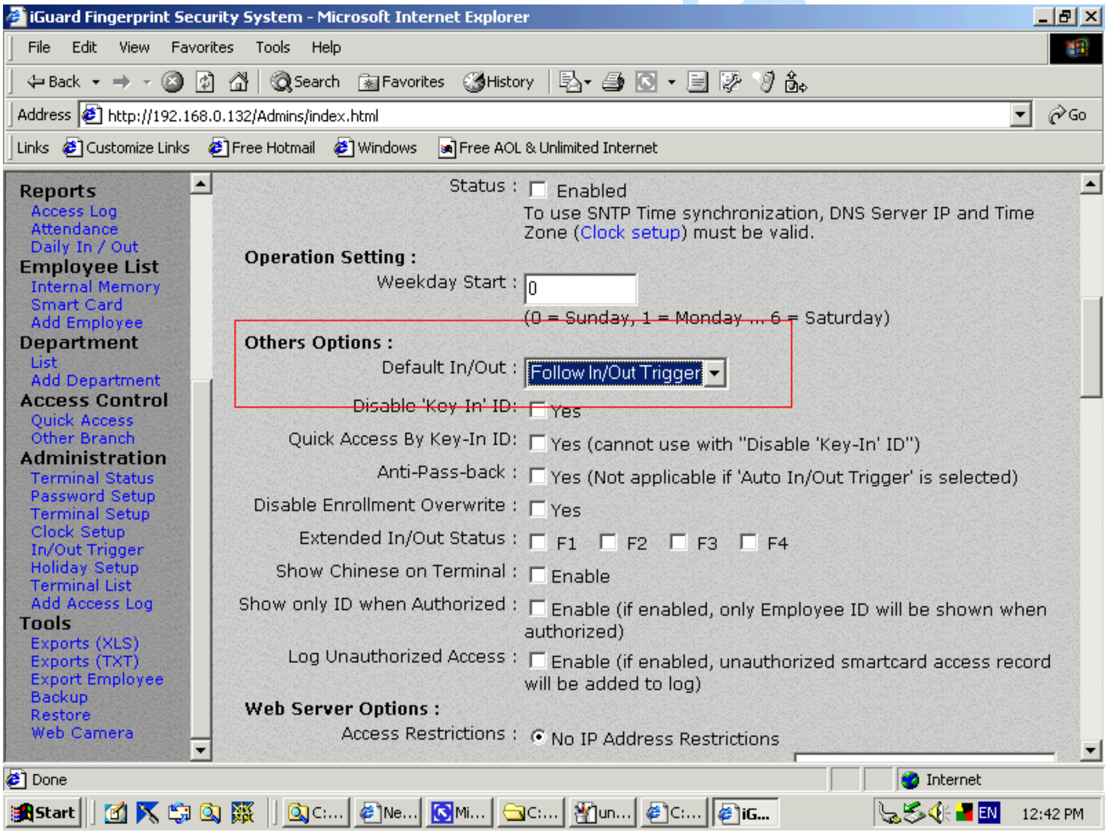
©2001 Lucky Technology. All rights reserved.

7.2 Various In/Out Modes

These functions will not be included in the standard LM series. Please contact our sales.

Different Modes	**Description**
Follow IN/OUT Trigger (default)	If the default value is chosen, the IN/OUT setting will be defined in the In/Out Trigger Setup (see section Administration- IN/OUT Trigger)
Always Out	This will set the iGuard to show and record all attendance as "OUT".
Always In	This will set the iGuard to show and record all attendance as "IN".
Don't Show	This will set the iGuard to show and record all attendance as "IN".
Auto In/Out Trigger	This will automatically rotate between IN and OUT for users.
Extended In/Out Status	In addition to IN and OUT labels, 4 extra labels F1,F2,F3, and F4 can be selected manually using <-- button. In the access log, these labels will be shown accordingly. In some applications, these labels can be used as job code.

Select "terminal setup" in Internet browser, "Default In/Out" can be setup to various modes:



Status : ☐ Enabled
To use SNTP Time synchronization, DNS Server IP and Time Zone (Clock setup) must be valid.

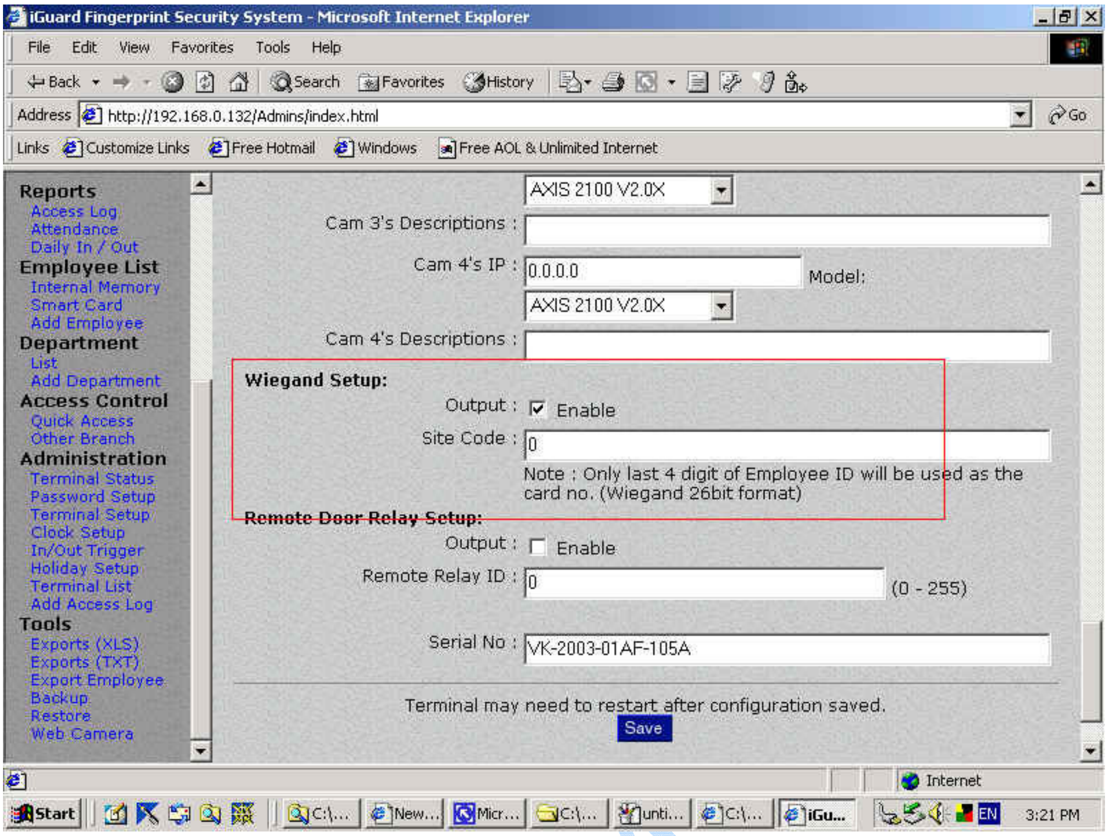
Operation Setting :
Weekday Start : 0
(0 = Sunday, 1 = Monday ... 6 = Saturday)

Others Options :
Default In/Out : Follow In/Out Trigger
Disable 'Key-In' ID: ☐ Yes
Quick Access By Key-In ID: ☐ Yes (cannot use with "Disable 'Key-In' ID")
Anti-Pass-back : ☐ Yes (Not applicable if 'Auto In/Out Trigger' is selected)
Disable Enrollment Overwrite : ☐ Yes
Extended In/Out Status : ☐ F1 ☐ F2 ☐ F3 ☐ F4
Show Chinese on Terminal : ☐ Enable
Show only ID when Authorized : ☐ Enable (if enabled, only Employee ID will be shown when authorized)
Log Unauthorized Access : ☐ Enable (if enabled, unauthorized smartcard access record will be added to log)

Web Server Options :
Access Restrictions : ● No IP Address Restrictions

7.3 Wiegand 26 bits Output

There is a Wiegand output connector at the back of iGuard and data with Wiegand 26 bits format can be enabled in the terminal setup.



AXIS 2100 V2.0X

Cam 3's Descriptions :

Cam 4's IP : 0.0.0.0 Model: AXIS 2100 V2.0X

Cam 4's Descriptions :

Wiegand Setup:

Output : ☑ Enable

Site Code : 0

Note : Only last 4 digit of Employee ID will be used as the card no. (Wiegand 26bit format)

Remote Door Relay Setup:

Output : □ Enable

Remote Relay ID : 0 (0 - 255)

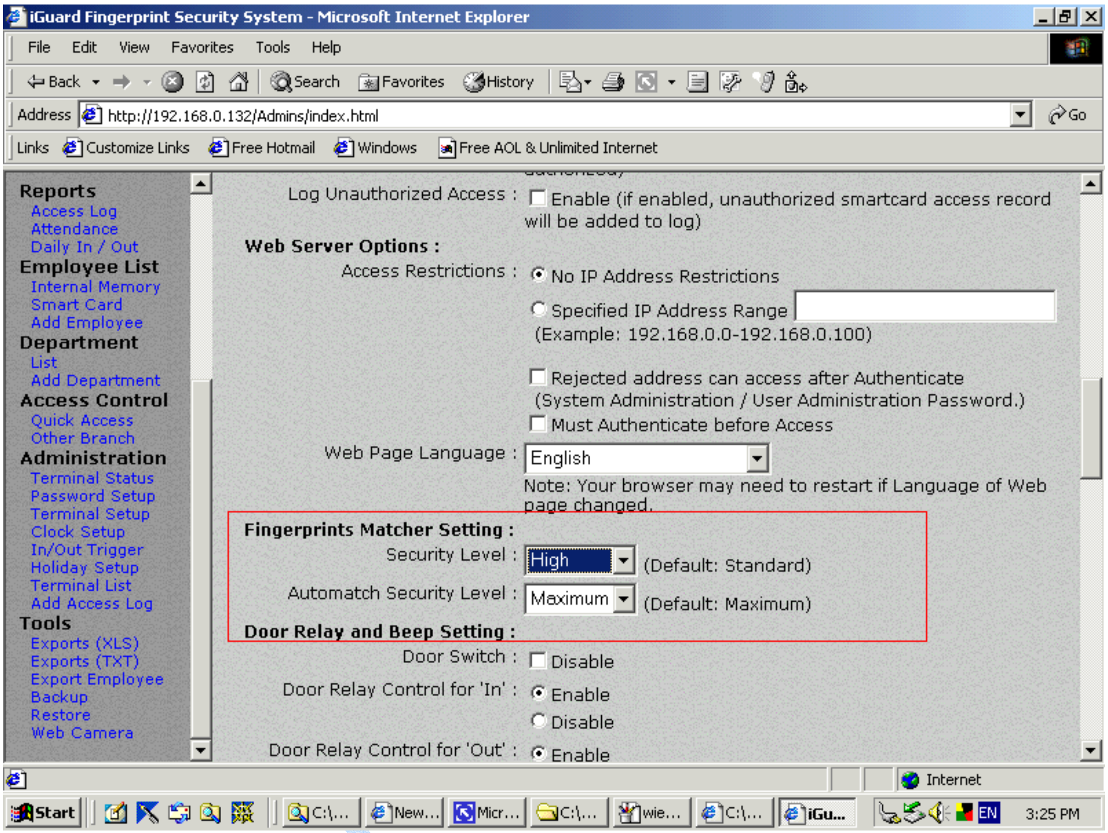
Serial No : VK-2003-01AF-105A

Terminal may need to restart after configuration saved.

7.4 Fingerprint and Automatch Matching Security

This option enables the administrator to set the level of security for fingerprint matching. Set it to low for normal application. If you need to use the device where high security is required, set this security to "high". However, it should be noted that a higher false rejects rate should be expected.

Go to Terminal Setup:



Log Unauthorized Access : ☐ Enable (if enabled, unauthorized smartcard access record will be added to log)

Web Server Options :

Access Restrictions : ● No IP Address Restrictions
○ Specified IP Address Range
(Example: 192.168.0.0-192.168.0.100)

☐ Rejected address can access after Authenticate (System Administration / User Administration Password.)
☐ Must Authenticate before Access

Web Page Language : English
Note: Your browser may need to restart if Language of Web page changed.

Fingerprints Matcher Setting :

Security Level : High (Default: Standard)
Automatch Security Level : Maximum (Default: Maximum)

Door Relay and Beep Setting :

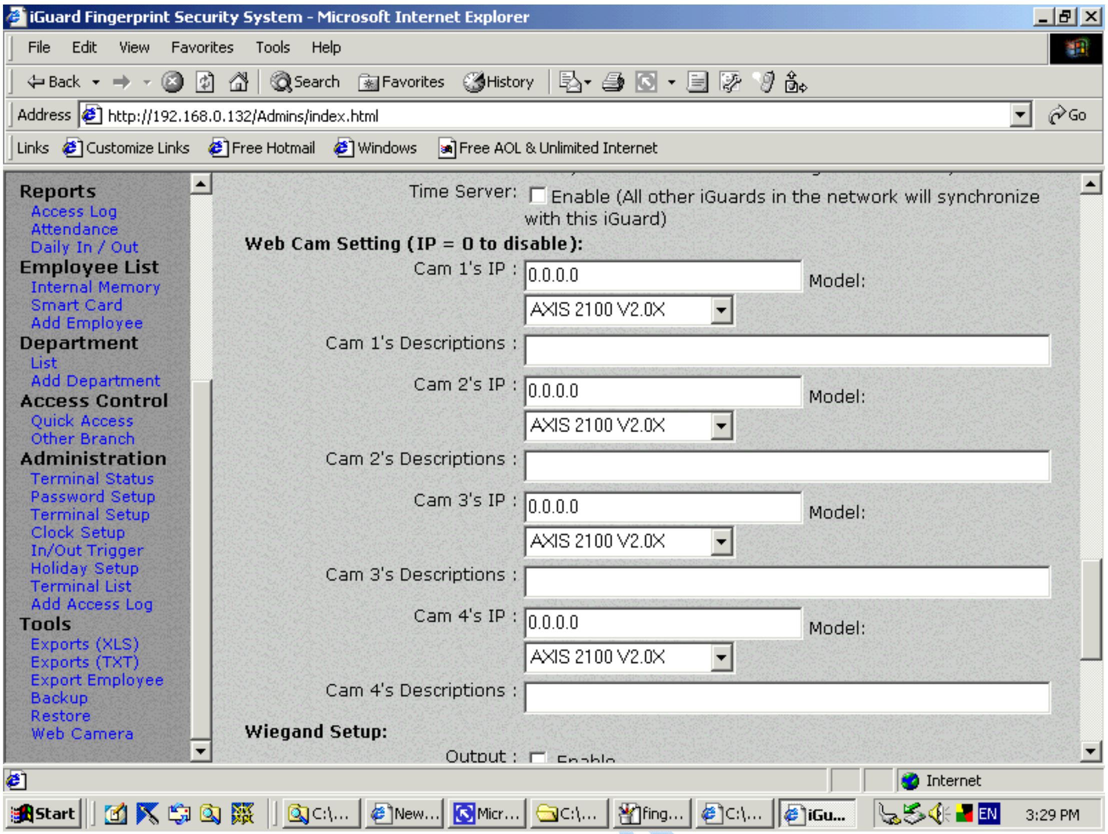
Door Switch : ☐ Disable
Door Relay Control for 'In' : ● Enable
○ Disable
Door Relay Control for 'Out' : ● Enable

7.5 Web Camera Link Setup

Web-Cam Settings

You can use the device to re-direct your web camera's pictures to the outside world. Currently the only supported web cameras are *Axis 2100 Network Camera* from *Axis Communications* and Network Camera from *JVC*. Up to four web cameras are supported.

In the terminal setup, type in the IP addresses of the Web Cameras and select the Web Camera model number.



Time Server: □ Enable (All other iGuards in the network will synchronize with this iGuard)

Web Cam Setting (IP = 0 to disable):

Cam 1's IP : 0.0.0.0 Model: AXIS 2100 V2.0X

Cam 1's Descriptions :

Cam 2's IP : 0.0.0.0 Model: AXIS 2100 V2.0X

Cam 2's Descriptions :

Cam 3's IP : 0.0.0.0 Model: AXIS 2100 V2.0X

Cam 3's Descriptions :

Cam 4's IP : 0.0.0.0 Model: AXIS 2100 V2.0X

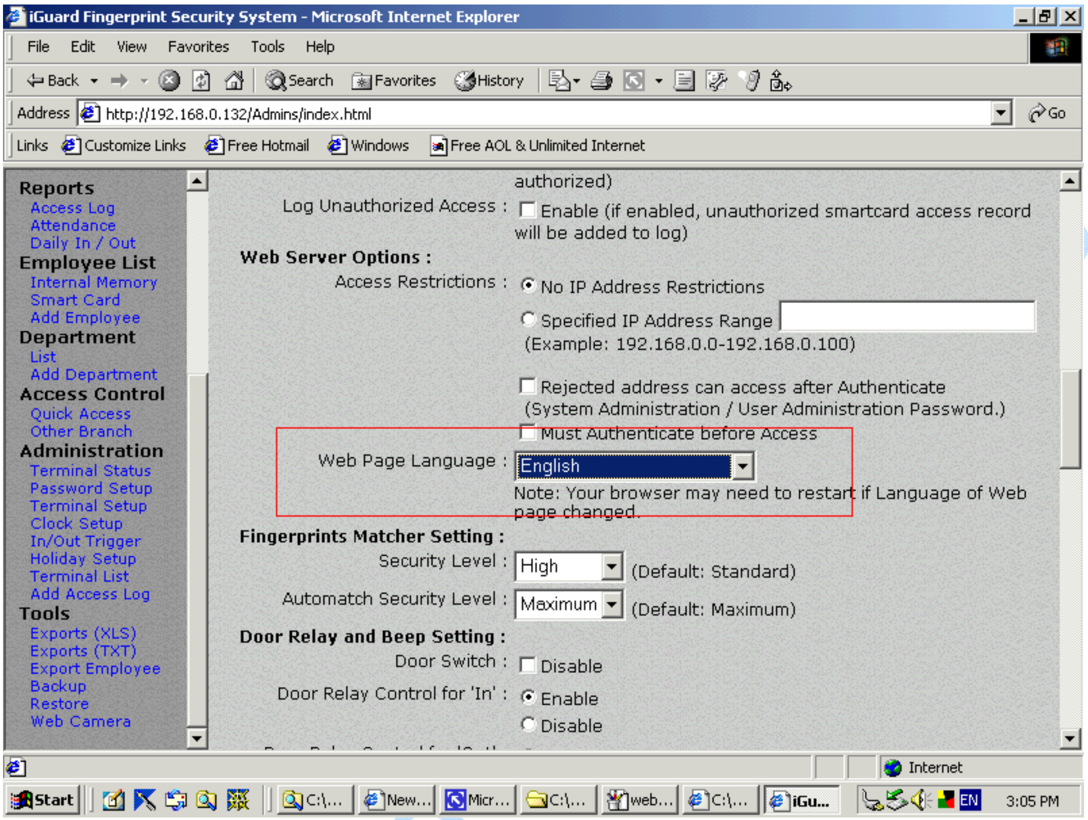
Cam 4's Descriptions :

Wiegand Setup:

Output : □ Enable

7.6 Web Pages Languages

The language used in web administration pages can be changed. Currently few languages are supported: English, Simplified Chinese, Traditional Chinese, and Japanese. Contact our sales if you want to incorporate your languages.



Address http://192.168.0.132/Admins/index.html

authorized)

Log Unauthorized Access : □ Enable (if enabled, unauthorized smartcard access record will be added to log)

Web Server Options :

Access Restrictions : ● No IP Address Restrictions

○ Specified IP Address Range

(Example: 192.168.0.0-192.168.0.100)

□ Rejected address can access after Authenticate (System Administration / User Administration Password.)

□ Must Authenticate before Access

Web Page Language : English

Note: Your browser may need to restart if Language of Web page changed.

Fingerprints Matcher Setting :

Security Level : High (Default: Standard)

Automatch Security Level : Maximum (Default: Maximum)

Door Relay and Beep Setting :

Door Switch : □ Disable

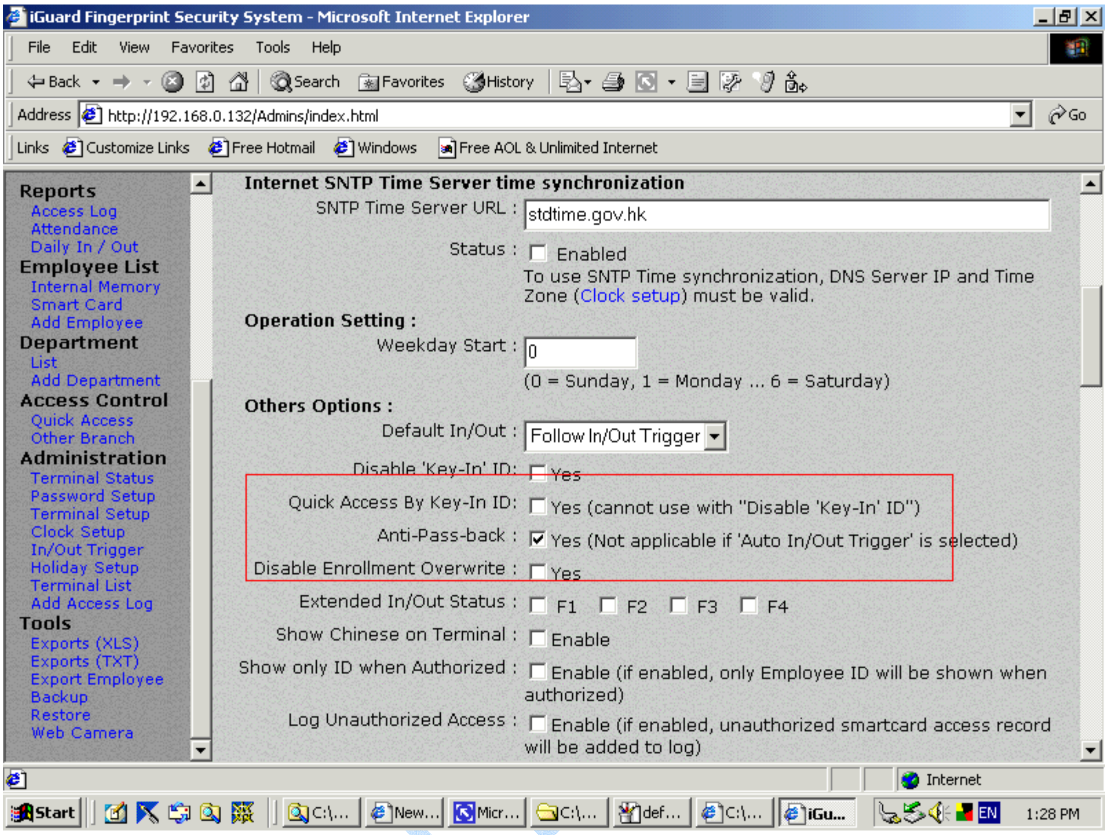
Door Relay Control for 'In' : ● Enable

○ Disable

7.7 Anti-Passback

This function is not available in the standard LM Series. Please contact our sales.

Anti-Passback	When enabled, this feature prevents the same employee to enter the premises twice if he/she has not checked out.



Internet SNTP Time Server time synchronization

SNTP Time Server URL : stdtime.gov.hk

Status : □ Enabled
To use SNTP Time synchronization, DNS Server IP and Time Zone (Clock setup) must be valid.

Operation Setting :

Weekday Start : 0
(0 = Sunday, 1 = Monday ... 6 = Saturday)

Others Options :

Default In/Out : Follow In/Out Trigger

Disable 'Key-In' ID: □ Yes

Quick Access By Key-In ID: □ Yes (cannot use with "Disable 'Key-In' ID")

Anti-Pass-back : ☑ Yes (Not applicable if 'Auto In/Out Trigger' is selected)

Disable Enrollment Overwrite : □ Yes

Extended In/Out Status : □ F1 □ F2 □ F3 □ F4

Show Chinese on Terminal : □ Enable

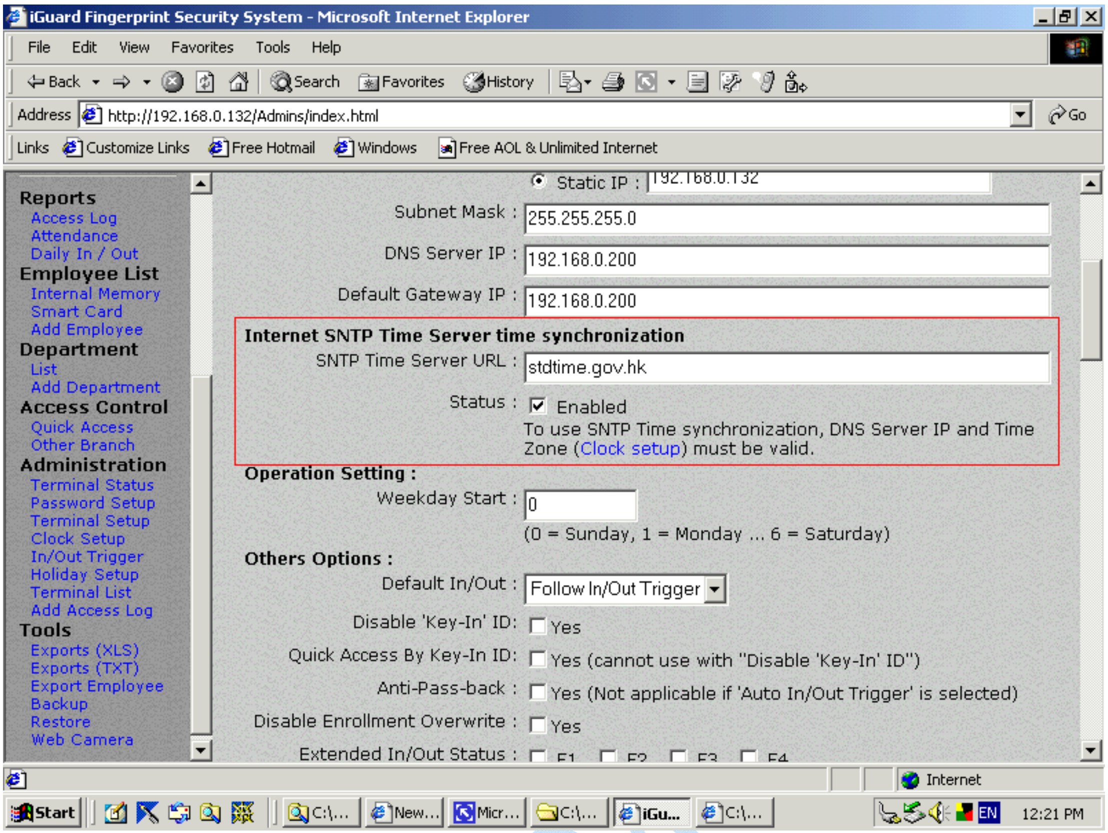
Show only ID when Authorized : □ Enable (if enabled, only Employee ID will be shown when authorized)

Log Unauthorized Access : □ Enable (if enabled, unauthorized smartcard access record will be added to log)

7.8 SNTP Time Server

Internet SNTP Time Server time synchronization

Go to Terminal Setup:



● Static IP : 192.168.0.132

Subnet Mask : 255.255.255.0

DNS Server IP : 192.168.0.200

Default Gateway IP : 192.168.0.200

Internet SNTP Time Server time synchronization

SNTP Time Server URL : stdtime.gov.hk

Status : ☑ Enabled

To use SNTP Time synchronization, DNS Server IP and Time Zone (Clock setup) must be valid.

Operation Setting :

Weekday Start : 0

(0 = Sunday, 1 = Monday ... 6 = Saturday)

Others Options :

Default In/Out : Follow In/Out Trigger

Disable 'Key-In' ID: □ Yes

Quick Access By Key-In ID: □ Yes (cannot use with "Disable 'Key-In' ID")

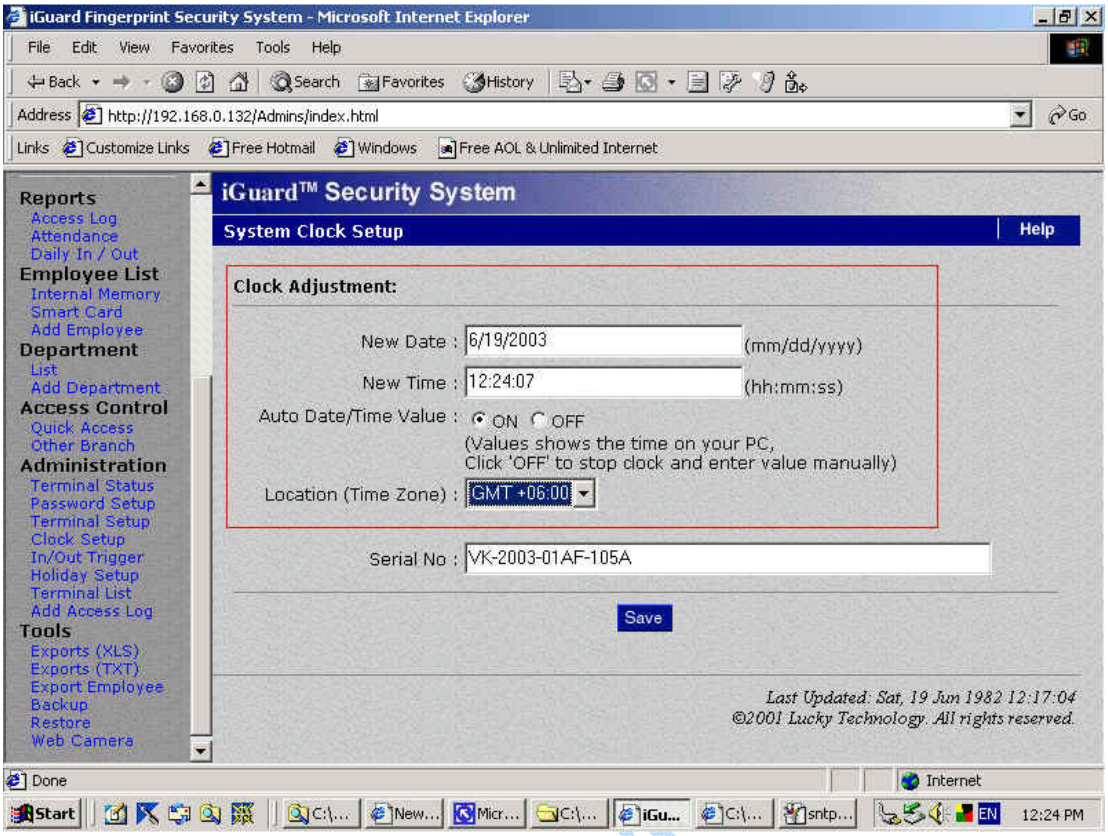
Anti-Pass-back : □ Yes (Not applicable if 'Auto In/Out Trigger' is selected)

Disable Enrollment Overwrite : □ Yes

Extended In/Out Status : □ F1 □ F2 □ F3 □ F4

SNTP Time Server URL: This should be set to the standard time on the Internet. It is represented by the Greenwich Time. To enable it you musts check the checkbox of the "Status" Field. Once you have selected this, you should go to the Clock Setup under Administration to adjust the Greenwich Time to your local time by +/- from the default GMT.

Status: To enable the SNTP time server, you should check this box and make sure to set up the DNS Server IP and Time Zone under "Clock Setup" appropriately.



iGuard™ Security System

System Clock Setup

Clock Adjustment:

New Date : 6/19/2003 (mm/dd/yyyy)

New Time : 12:24:07 (hh:mm:ss)

Auto Date/Time Value : ● ON ○ OFF
(Values shows the time on your PC,
Click 'OFF' to stop clock and enter value manually)

Location (Time Zone) : GMT +06:00

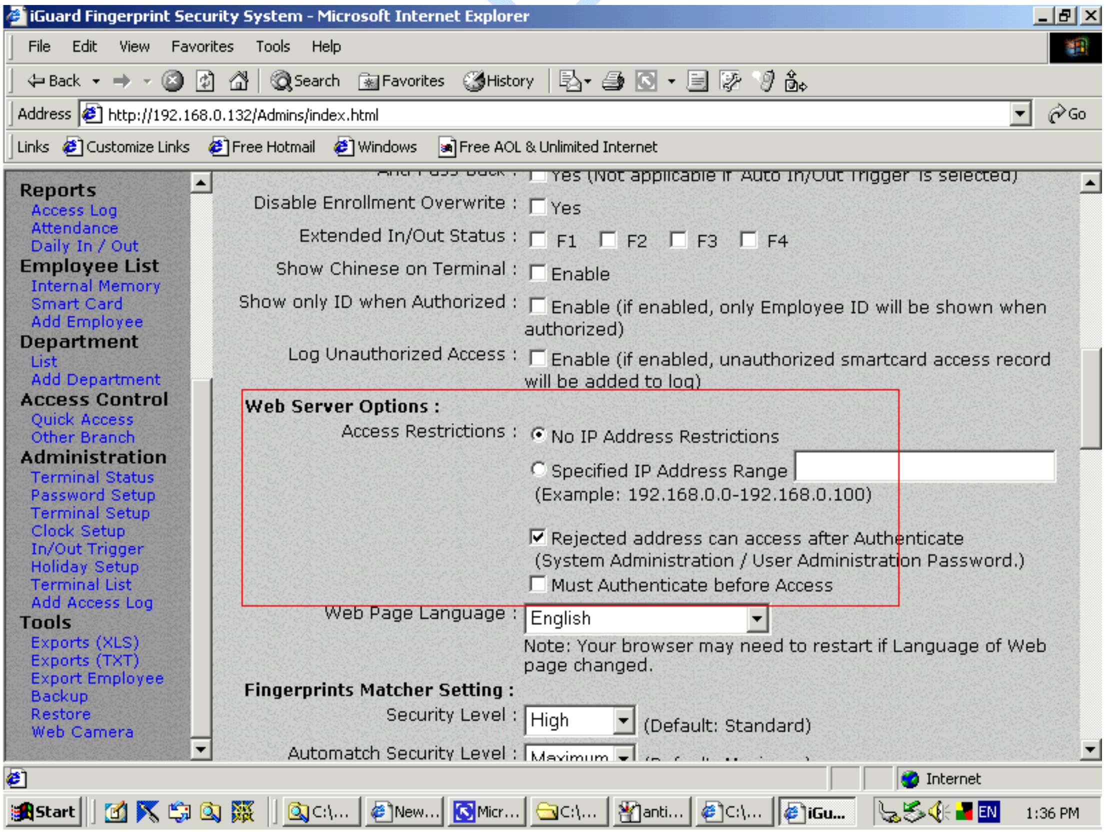
Serial No : VK-2003-01AF-105A

Last Updated: Sat, 19 Jun 1982 12:17:04
©2001 Lucky Technology. All rights reserved.

7.9 Security for Web Access

Setup Security for Web Administration Access

No IP Address Restrictions	There is no restriction to access the web administration page from any PC's or any users.
Access Restriction	An IP address or a range of IP address can be set with a right of accessing the web administration page. e.g. 203.80.62.2-203.80.62.8. PC's with IP address falls out of the IP address or range of IP addresses will not be able to access the web administration page.
Rejected address can access after Authenticate	Check this box if you still want to allow outsiders to access the device even if the IP address is out of the specified range discussed above. The device will ask for the administrator password for granting the access. It is useful if you want to access the device remotely (such as in another country).
Must Authenticate before Access	Normally only the pages that involve changing the configuration & users' information require password. Check this box if you want to configure the device to ask for password for all pages.



Anti-Pass Back : □ Yes (Not applicable if Auto In/Out Trigger is selected)

Disable Enrollment Overwrite : □ Yes

Extended In/Out Status : □ F1 □ F2 □ F3 □ F4

Show Chinese on Terminal : □ Enable

Show only ID when Authorized : □ Enable (if enabled, only Employee ID will be shown when authorized)

Log Unauthorized Access : □ Enable (if enabled, unauthorized smartcard access record will be added to log)

Web Server Options :

Access Restrictions : ● No IP Address Restrictions

○ Specified IP Address Range
(Example: 192.168.0.0-192.168.0.100)

☑ Rejected address can access after Authenticate
(System Administration / User Administration Password.)

□ Must Authenticate before Access

Web Page Language : English

Note: Your browser may need to restart if Language of Web page changed.

Fingerprints Matcher Setting :

Security Level : High (Default: Standard)

Automatch Security Level : Maximum

7.10 Reset Device

If you want to erase all the users information and access records stored in the iGuard internal memory, and to reset all the settings to the factory defaults, you can perform the System Reset function to clear all the stored data. There are two databases inside the iGuard: User Database & Access Database. The User Database stores the user information, including the fingerprint data & the access rights. It also stores the department information. The Access Database only stores the Access records. It does not contain any user information.

You can selectively delete any one or both databases. It is done by selecting "**Function 7**" in the setup menu, as shown in the following: -

Description	***LCD Display***
While in Standby Mode, press the **Func** key to enter the Setup Menu. You will be prompted to enter the Administrator Password (default: 123) as shown.	Enter Password: _
Press the **Func** key to continue, then select **Function 7** to enter the System Shutdown/Reset menu.	Press 7: System Shutdown/Reset
You will be asked if you want to delete the User Database. Enter **1** if you want to clear all the existing User Information, or else press **2** to keep the existing information.	Reset User Dbase Yes/No (1/2)? _
Then, you will be asked if you want to delete the Access Database. Enter **1** if you want to clear the log, and enter **2** if you want to keep it.	Reset Access log Yes/No (1/2)? _
Finally, you will then be asked if you want to reset the settings to the factory default. Enter **1** if you want to reset the device to its factory default (such as resetting the IP address to the default 192.168.0.200).	Factory Default Yes/No (1/2)? _
The system will perform a system reset, and then it will return to the standby mode (it usually takes around 20 seconds).	Mon 30 Dec 13:49 ID #:_

Note:

In the unlikely event that your iGuard does not function properly for some unknown reasons, you may also want to use this *System Shutdown/Reset* function to reset all the existing records in the machine.

7.11 Test Mode

Under normal operation, iGuard records all the user transactions in its Access Log. However, you can set the machine to ***Test Mode***, and it will temporary disable the machine from recording the transactions. This feature is useful when you have finished a new enrollment for a new user, and you want the new user to practice with the device.

You use "**Function A**" in the setup menu to toggle between Test Mode and Normal Mode, and is illustrated in the following steps:

Description	***LCD Display***
While in Standby Mode, press the **Func** key to enter the Setup Menu. You will be prompted to enter the Administrator Password (default: 123) as shown.	`Enter Password: _`

Press the **Func** key, then press "**A**" to toggle the machine to Test Mode. The Display will show the Test Mode status as shown. You can now ask the new users to practice with the machine, and the transactions will not be recorded.	`== Test Mode! ==`
	`ID #:_`

Following the same procedure above and press "**A**" again in the setup menu to put the machine back to Normal Mode.	`Mon 30 Dec 13:49`
	`ID #:_`

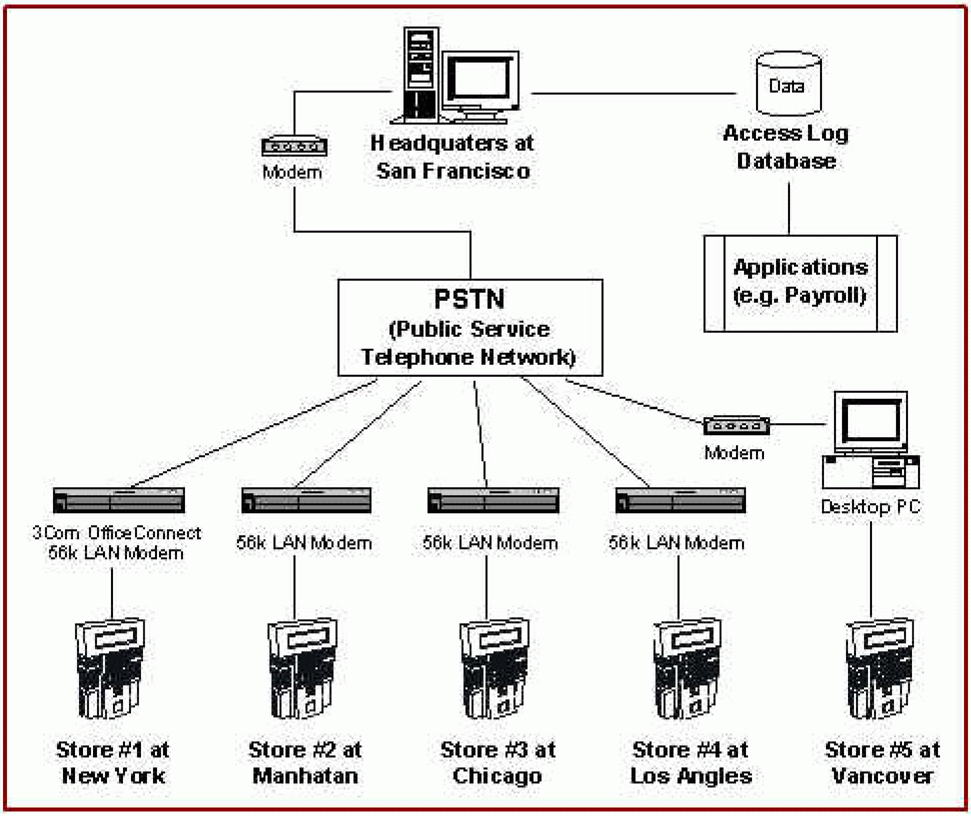
Note:

Please note that you must change the machine back to Normal Mode, or else the records in the access log will become invalid.

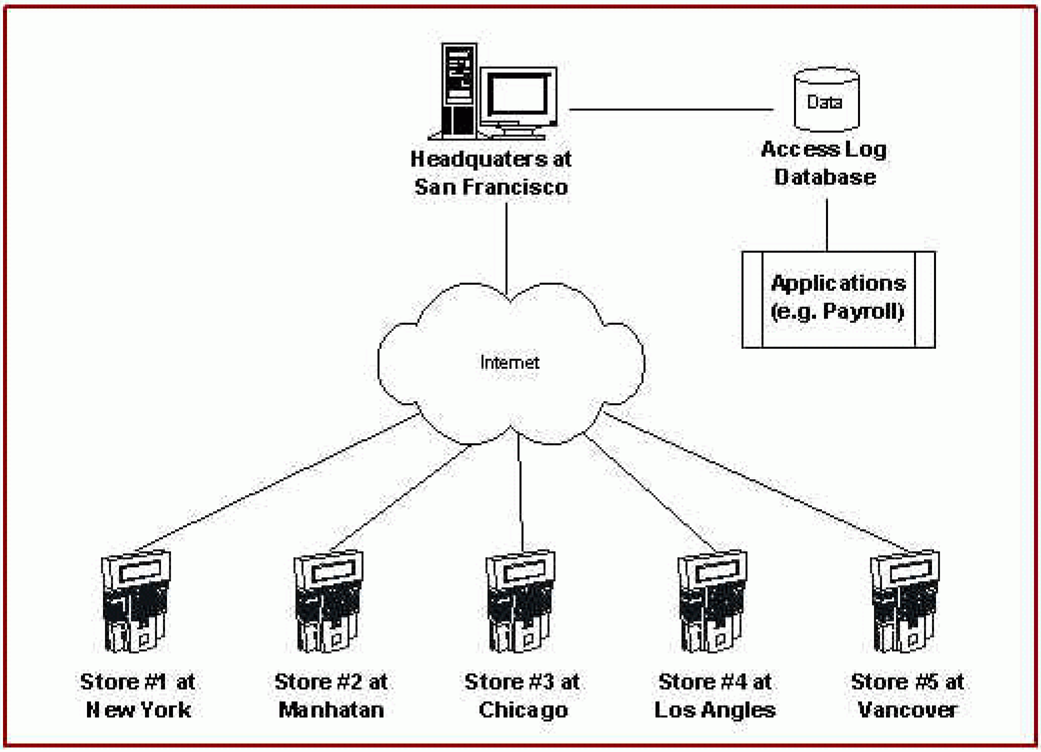
8 Appendix

Network Connection

1. Connection with PSTN

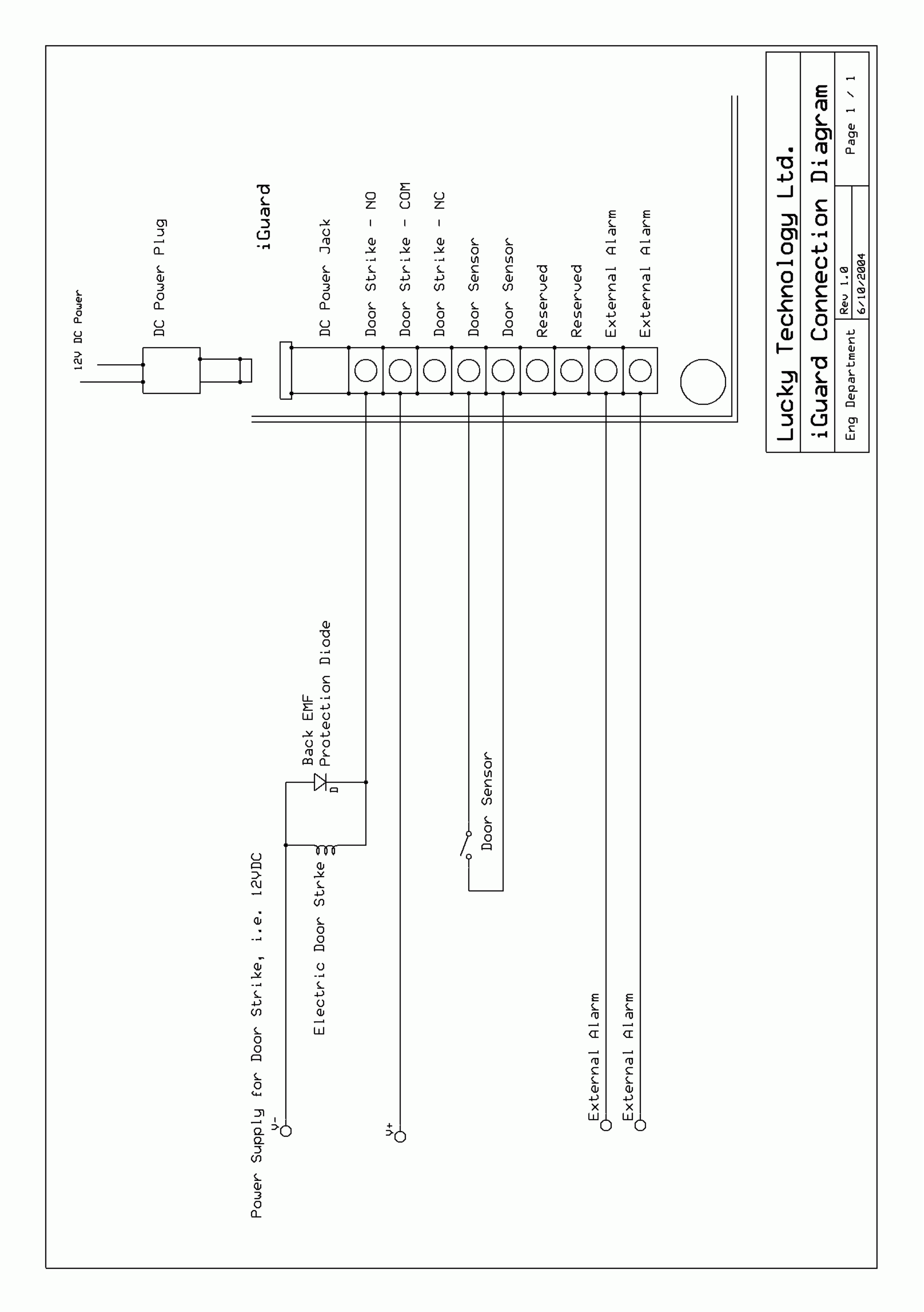


2. Connect with Internet

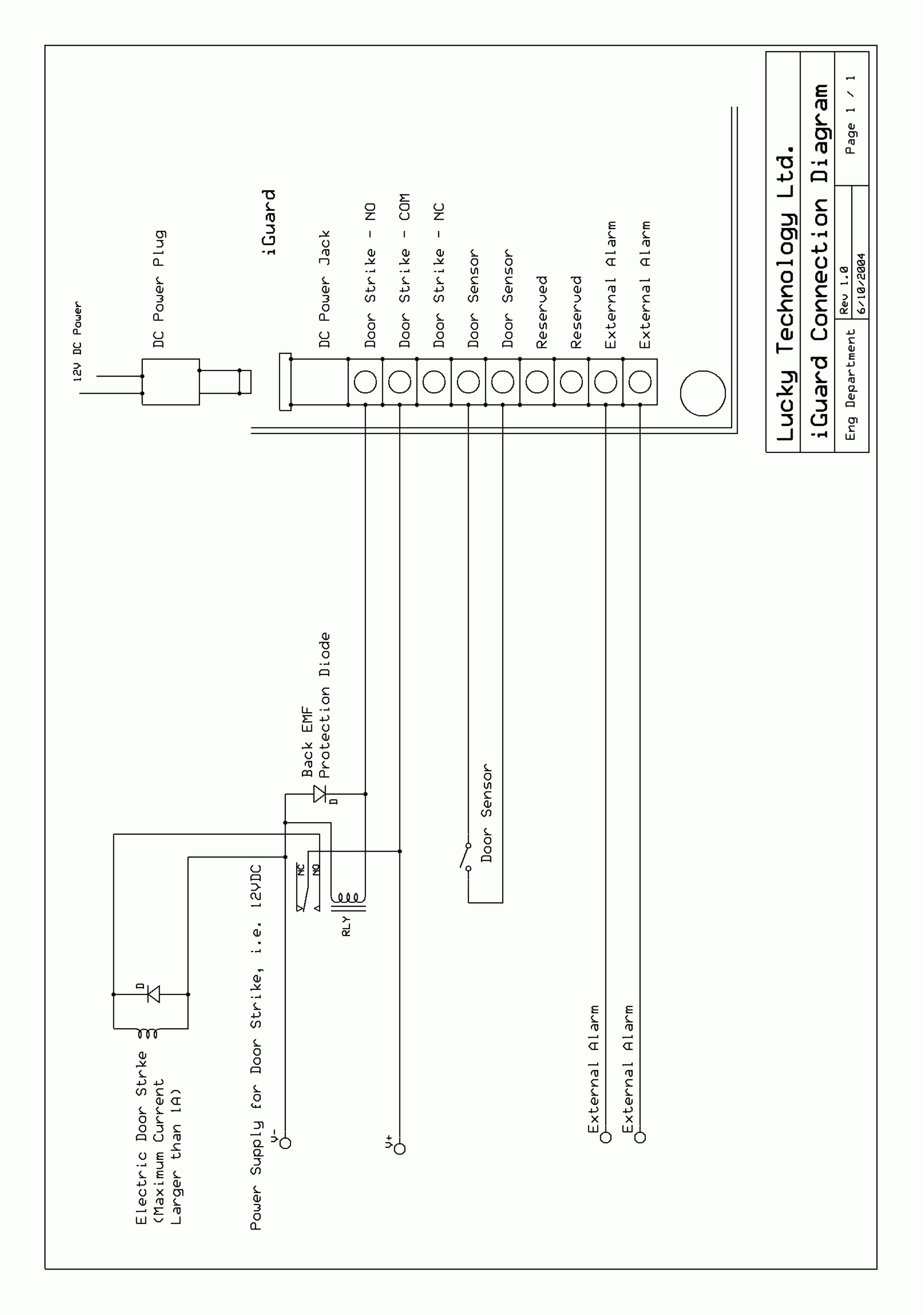


Connection Diagrams

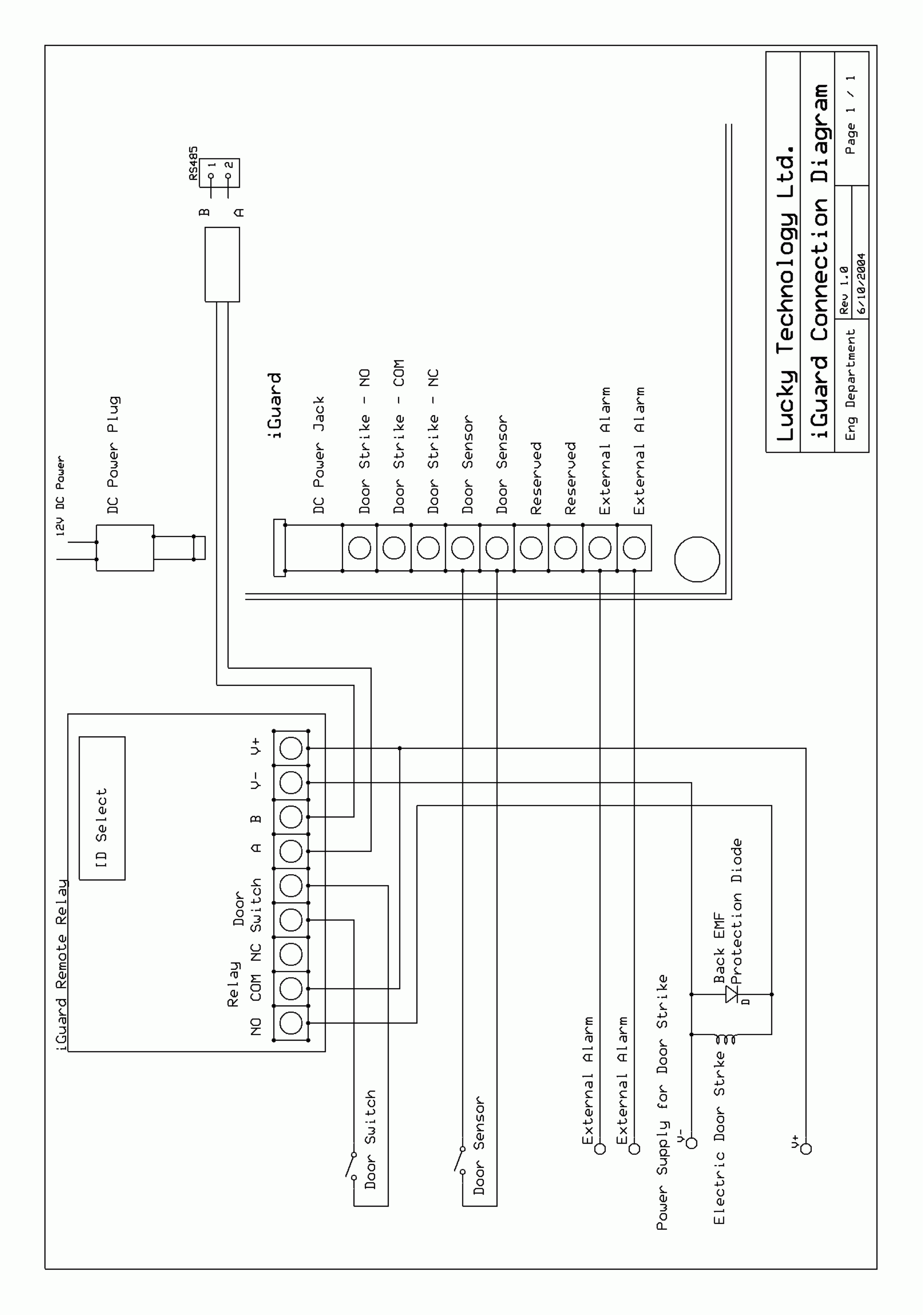
1. Basic Connection



2. Basic Connection (Large Load)



3. Connection Diagram – Remote Relay



End