iGuard FPS110

Operation Manual

Manual Version 3.33

Information to user: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

TABLE OF CONTENTS

YOUR NEW IGUARD FPS110 SYSTEM

Your new iGuard FPS110 Access Control / Time Attendance System combines ease of use and a wide range of features.

Fingerprint Identification:

- Incorporates the most advanced solid-state Capacitive Fingerprint Sensor[1] -- more reliable & compact than traditional optical sensor,
- Eliminates the reliability problems associated with optical sensor, such as edge distortion & mis-aligned optics, thus improve the quality of the fingerprint image.
- Two-finger enrollment – primary & secondary fingers.
- High false acceptance rate – less than 0.01%.
- All records are irrefutable and cannot be forged or altered.

Built-in Contactless SmartCard Reader (optional):

- Uses the most well proven Philips Mifare platform.
- User information, including the fingerprint information & access rights, is stored in the card rather than in the device, for maximum security.
- Enables quick-access operation by just presenting the smart card during normal office hours, where only low security is required.
- For maximum security, users can be verified by both the smart card and fingerprint image together.

Built-in Internet Web Server:

- Enables the device to attach directly to the existing corporate network using standard RJ-45 cabling, without the need for any dedicated PC.
- Allows the device to be accessed and managed easily by standard Internet Browser, such as Microsoft Internet Explorer and Netscape Navigator.
- Allows simultaneous access to various reports by many people at the same time.
- 100% stand-alone & self-contained – there is no need to connect to a main unit or occupy a dedicated computer.

As an Access Control System:

- Access Time restriction – you can define the authorized time for each individual or for a group of individuals.
- Terminal restriction – you can specify who has the rights to access a particular terminal. It is useful in a multi-device environment, where multiple doors are controlled by different devices.

[1] Veridicom – http://www.veridicom.com

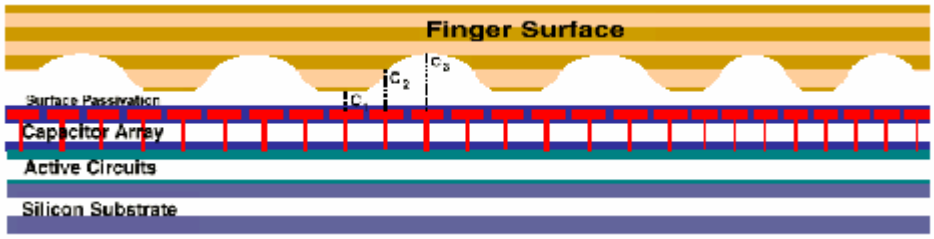
- Password / Fingerprint Access – you can define the period in which password can be used instead of fingerprint for access. This is particularly useful if you want to just use password to access during normal office hours, but to restrict the access to authorized people only after office hours.

As a Time Attendance System:

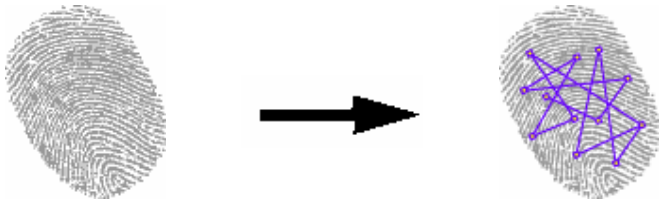
- Default Clock-In & Clock-Out time – you can setup the default clock-in time & clock-out time, so the user does not need to specify every time when he/she clocks in & out.
- Totally eliminate the buddy-punching problems & other frauds.

HOW IT WORKS?

iGuard FPS110 uses a solid-state sensor that images fingerprints by measuring capacitance. Its rugged, silicon-based design offers substantial advantages over optical-based sensors.



Beneath the sensor's surface passivation layer is a 300 x 300 array of capacitor plates (90,000 capacitors) spaced with a 50 mm pitch. The diagram above shows that the ridges and valleys of the fingerprint at different distances from the capacitor plates. That difference corresponds to a capacitance difference measured by the sensor. An on-board analog-to-digital converter converts each capacitance measurement into an 8-bit digital value, and then forms the fingerprint image. The system then extracts a set of characteristics unique to that fingerprint, called minutia. This minutia data uniquely identifies an individual.



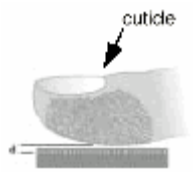
Raw Image Extracted Minutiaes

A NOTE ON FINGERPRINT IMAGE

iGuard incorporates the advanced DFX (Difficult Fingerprint Extraction) technology (originally developed by Bell Labs USA), and works very well with most people's fingerprint images, and iGuard can achieve a very low false-reject-rate (1%). However, as individuals, our hands have different levels of moisture. In some cases, iGuard may have difficulty in recognizing people's fingerprint, especially for the people with very dry skin. The problem is more noticeable during the enrollment process, where the product requires a more accurate and higher quality fingerprint image than the normal verification process. The easiest way to get around with this problem is to apply a very small amount of skin moisturizing lotion to the thumbs during the enrollment process. In most cases, this extra step is only required during the enrollment process, and is not necessary in the daily verification process.

Hints for Capturing Fingerprint Images

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



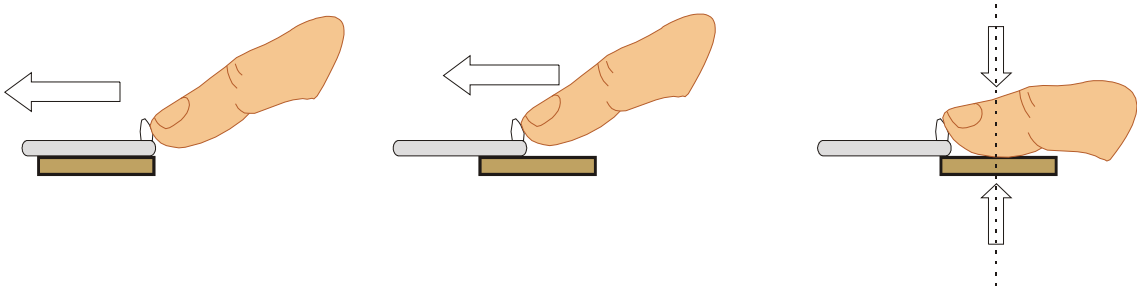
The Core

The Tip

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

The fingerprint sensor shutter

There is a shutter that covers the fingerprint sensor, which serves to protect the surface of the sensor. When you lift the shutter with your thumb, make sure to lift it all the way up to the top. It is because the device has a sensor that senses the position of the shutter, and the device won't start capturing the fingerprint until the shutter is lifted all the way up. ***Note***: it may take some practices to align the core of the fingerprint to the center of the sensor while lifting the shutter up.



SAFETY PRECAUTIONS

- This product has been designed as an 'indoor' device. Do not install and operate the product outdoors.

- If used an access control device, it is advised to select the type of door strike that will automatically release the door lock when power failure occurs. This is for safety purpose when, for example, a fire occurs and the electric power is interrupted, the people can still get out of the premises.

OPERATION MODES

Your iGuard system can be configured to different operation modes:

- Access Control Mode / Time Attendance Mode
- Master Mode / Slave Mode.
- Test Mode / Normal Mode.

The default operation modes are **Access Control Mode** & **Master Mode**. This section explains the difference between these modes. Please note that you must use the Internet Browser (discussed later) to change the first two operation modes. The "Test Mode" is for allowing new users to practice with the machine, and will be discussed in detail in the section **"Advanced Feature – Test Mode"** later.

Access Control Mode vs. Time Attendance Mode

The Access Control Mode is to control the employees from accessing the business premises. The system controls the electronic door strike to lock / unlock the door. You can assign users to different departments, and you can control the authorized time for the members in each department. For example, if the authorized time for access for the Marketing Department is from 9:00am to 6:00pm, Monday to Saturday, then all the members in this department can only get into the office within this authorized time period.

In a multi-device environment, you can further assign the access rights for each department in accessing different terminals. For example, you can allow only the members of the Marketing Department to enter the main office, and restrict all other employees not belong to this department from getting into the office, even though it is within the authorized period.

You can also use the Access Password discussed above to gain access & by-pass the fingerprint verification procedure. Please note that you can use the *Password Access* page found in the Internet Browser Main Page to control the time restriction of this operation.

The Time Attendance Mode is used to record the Clock In / Clock Out time of the employees, and it is very useful to avoid the buddy-punching problem. The major difference is that in this mode, the device is not used to control the door strike, and there is no time & terminal restriction.

Master Mode 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. This process is called enrollment, and it can be done in any device, including both Master and Slave devices. The user data will than 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 authenticate in any of these devices.

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 access the Master device, using the Internet Browser, to obtain all the access and attendance records of the whole system. It is not necessary to access the Slave devices.

INSTALLING YOUR IGUARD FPS110

Power Requirements

iGuard FPS110 requires an 12V DC/800mA(or above) Switching Power Supply. Although most Door Strikes in the market also use 12V DC to operate, we suggest that do not share the same power supply with other device such as Door Strike.

Deciding where to install

iGuard is a wall-mounted unit with a very small footprint, and can be conveniently installed anywhere. If used as an access control system, the product should be installed closely to the door, so the user can open the door within the timeout period after authentication (5 sec. by default). Also note the following points:

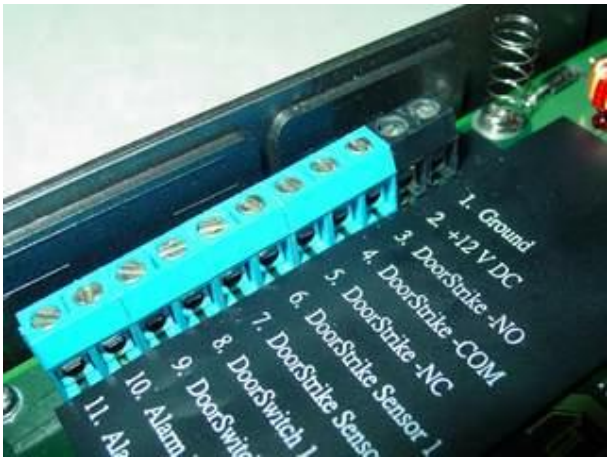
- Allow adequate air circulation to prevent internal heat buildup.
- Do not install the product next to heat sources such as air dusts, or in a place subject to direct sunlight and excessive dust.

Mounting the Metal Back Panel

The iGuard comes with a metal panel for mounting on the wall. For better performance, IT IS HIGHLY SUGGESTED TO CONNECT THE PANEL TO THE GROUND. It is because by grounding the system, the static charge that users may have can be discharged easily to the ground, and will help improving the fingerprint images of the users.

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.

Open Door Switch (optional):
Terminals #8 & #9. An optional door switch can be connected to these terminals. It is used to open the door remotely, such as opening the door from the inside of the business premises, or from the reception area.

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.

Connections – Corporate Network

You can connect iGuard FPS110 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 Internet Browser (such as Microsoft Internet Explorer & Netscape Navigator).

The connection is optional if the product is used solely as an Access Control System. However, some of the features must be setup and maintained via the Internet Browser (such as assigning the authorized time period for an individual to access). If you want to use the feature, you must connect the product to your corporate network.

If it is used as a Time Attendance System, you must connect iGuard FPS110 to the network, since the Internet Browser is required to retrieve the attendance records and reports.

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

POWER-UP

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

Description	***LCD Display***
1. Power Up -- when iGuard is power-up, it will perform a self-test…	`Initializing...`
2. After about 10 sec., the device will load the system program…	`iGuard Security` `Loading.....`
3. After loading the system program, iGuard will enter the standby mode and is now ready to use.	`Mon Aug 30 12:00` `ID #:_`

CONFIGURING YOUR IGUARD FPS110 (FUNCTION 5)

This section describes how to set the system date & time, the network & TCP/IP settings, passwords, and test your network connection. The administrator password is required for the system administrator to access the system menu and to configure the system parameters. *The default administrator password is 123.*

Setting the date and time

You need to enter the date and time so that iGuard FPS110 can time stamp all the access & time attendance records. Follow these steps to set the system date and time: -

Description	***LCD Display***
1. 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:` `_`
2. Enter the Administrator Password (e.g. 123).	`Enter Password:` `123_`

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

4. 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`
5. After pressing the **Func** key, the current time is displayed. Enter the new time then press the **Func** key to continue.	`Time (H:M:S):` `13:45:23`
6. The system will then ask for the name *(to be continued in the next section….)*.	`Name:` `_`

Note:
iGuard FPS110 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.

Setting the Network & TCP/IP address

You can connect iGuard FPS110 directly to your corporate network. You 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 we suggest that it is better to assign a static IP address to the product.

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***
1. *(…continue from the previous step)* Enter the name of the device (e.g., A123). A more meaningful & descriptive name, such as "Unit A", can be assigned using the setup pages in the Internet Browser (described in later sections).	Name: A123_
2. 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).	IP Address: 192.168.001.123_
3. Press **Func** key to continue. Enter the sub-net mask here (e.g., 255.255.255.0).	Subnet Mask: 255.255.255.000
4. Press **Func** key to continue. Enter the address of the Default Gateway (e.g., 192.168.1.200).	Default Gateway: 192.168.001.200_
5. Press **Func** key to continue. Enter the address of the Domain Name Server (e.g., 192.168.1.200).	DNS: 192.168.001.200_
6. Press **Func** key to continue. Enter the address of the WINS (e.g., 192.168.1.200).	WINS: 192.168.001.200_
7. Press **Func** key to continue. You will be asked if the device is a *Master* or *Slave* device.	Master/Slave: (1/2)? Master
8. iGuard FPS110 can be configured as Master or Slave device. It is used in a multi-device environment, where more than one iGuard are connected to the same network, and the information is shared among the devices. More details will be discussed later. Press **1** to select Master for now. The system will reset itself and will return to Standby Mode.	Mon Aug 30 13:46 ID #:_

Setting the Administrator Password & Access Password

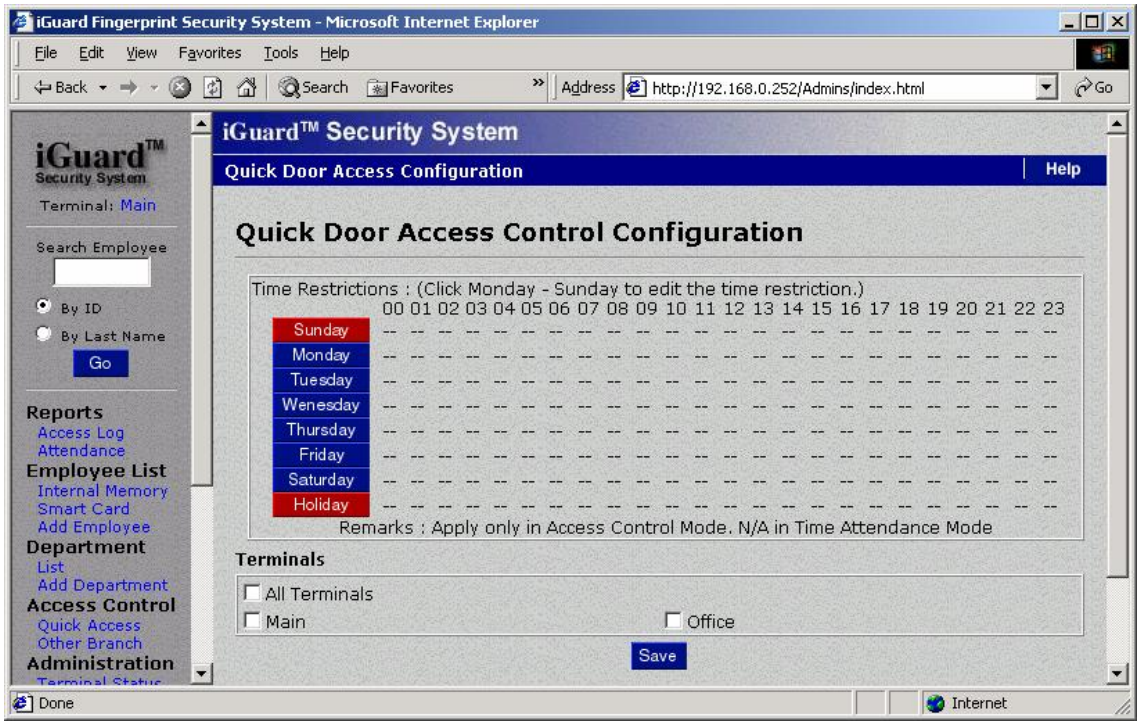
iGuard FPS110 has two *"global"* passwords[2]. The *Administrator Password* is used to access the system menu and to configure the system (such as accessing the setup menu in the last example). The *Access Password* is useful only when the device is configured as Access Control Mode (i.e., not configured as Time Attendance Mode). User can use this Access Password to gain access without verifying with the fingerprint image.

Follow these steps to assign & edit the two passwords:-

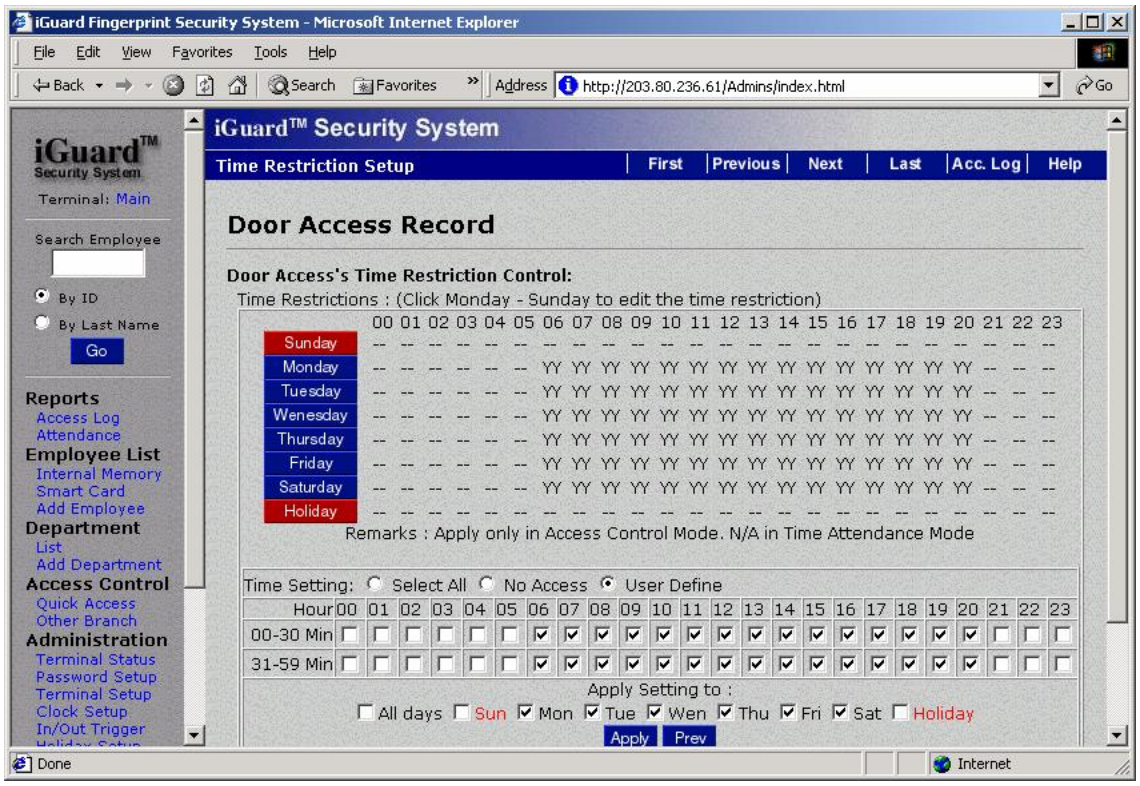
Description	***LCD Display***
1. While in Standby Mode, press the **Func** key to enter the Setup Menu. Enter the Administrator Password (default 123) and press **Func** key, then press **6** to select "Set Password…" menu.	Admin Password: 123_
2. Press the **backspace** to erase the old password, and enter the new password (e.g., AB456).	Admin Password: AB456_
3. Press the **Func** key to accept the new Administrator Password. You will then be prompted for the Access Password as shown.	Access Password: _
4. Enter the new Access Password (e.g., 9394AB709). It is suggested to use a long and hard-to-guess password (max 10 chars).	Access Password: 9394AB709_
5. Press **Func** to continue. The system will return to Standby Mode.	Mon Aug 30 13:49 ID #:_

Note:
You must enable the 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: -

[2] 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.



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: -



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

Description	***LCD Display***
1. Press the **Func** key while in the Standby Mode. You will then be asked to enter the password.	`Enter Password:` `_`
2. Enter the Access Password (such as 9394AB709). The password is shown as astride for security reason.	`Enter Password:` `*********_`
3. 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.

BASIC OPERATIONS

You can perform basic operations on the iGuard device, including fingerprint enrollment, activating & in-activating employees, and deleting employees, without using the Internet browsers. This section discusses these basic operations in detail.

Enrollment (Function 1)

During the enrollment process, a person's fingerprints are captured, and the information of the images is extracted and stored in the internal database for later verification. Each person must register two fingers: one as the primary and the other one as the secondary. In case when the primary finger is not suitable for verification (such as when the finger is hurt), the person can use his 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 & 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 data:-

Description	***LCD Display***
1. 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.	`Enter ID # and` `scan 1st Finger`
2. Enter the user ID # (e.g. A01). The ID can be of any length from 1 character to 10 characters.	`Enter ID # and` `A01_`

3. 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`
	`|||||||||||||||`

4. After the quality bar reaches the right end, you will be asked to remove the finger from the sensor.

```
Analyzing.  Pls
Remove Finger...
```

5. 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
```

6. 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
```

7. 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
```

8. 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
```

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

```
Mon Aug 30 13:49
ID #:_
```

Verification

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***

1. While in Standby Mode, key in the user ID number (e.g., A01).

```
Mon Aug 30 13:49
A01_
```

2. Lift the shutter and place either your primary 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.

```
Scanning...
A01_
```

```
:
:
```

```

Verifying...
```

3. If you are authenticated, the device will open the door, and will return to the Standby Mode.

```

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 ID first. This feature will be discussed later in this section.

Suspending / Resuming User (Function 2 / 3)

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***
1. 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 :` `_`
2. Enter the ID # you want to suspend (e.g., A01).	`Enter ID :` `A01_`

3. Press the **Func** key to confirm. The ID # is suspended, and the user can no longer be authenticated. The system will return to Standby mode.	`ID# A01`
	`Inactivated!`
	`:`
	`:`
	`Mon Aug 30 13:49`
	`ID #:_`

To resume a user ID, select function 3 ("Re-activate ID") in the setup menu in step 1 above, and follow the same procedure.

Please note that you can also use the Internet Browser to Inactivate and Re-activate the ID. It will be discussed in later sections.

Deleting ID (Function 4)

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

Description	*LCD Display*
1. 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:` `_`
2. Enter the ID # you want to delete (e.g., A01).	`ID to Delete:` `A01_`

3. Press the **Func** key to confirm. The ID # is deleted, and the user can no longer get access. The system will return to Standby mode.	`ID# A01`
	`Deleted!`
	:
	:
	`Mon Aug 30 13:49`
	`ID #:_`

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.

Resetting the device (Function 7)

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.).

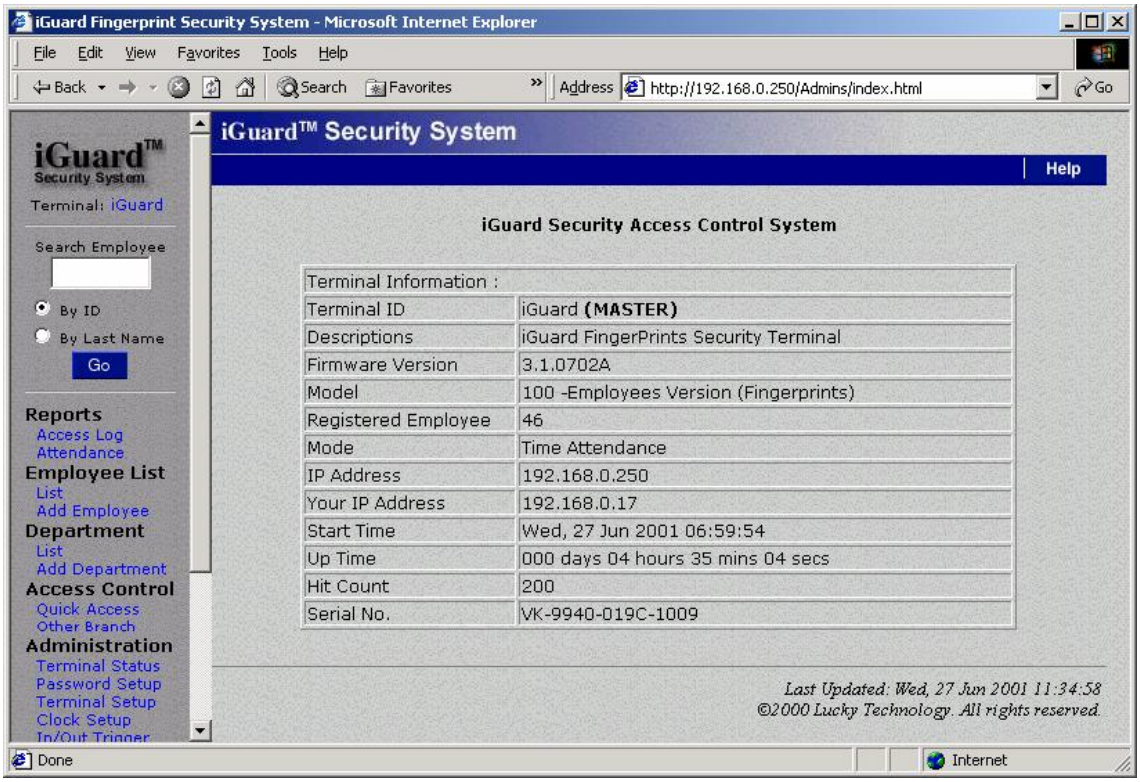
Auto – Match (Function 8)

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 (described in the next section).

USING THE INTERNET BROWSER

The built-in Web Server in each iGuard device allows you to use the popular Internet Browser software to manage & 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 in the Internet Browser (e.g., http://192.168.0.250). This is the IP address assigned to the device during the setup procedure. The following will appear in the browser: -



The iGuard's home page is divided into left & 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. For example, if your device comes with the optional SmartCard Reader, you will see more selections under the ***Employee List*** *section.*

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

Reports – Access Log

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

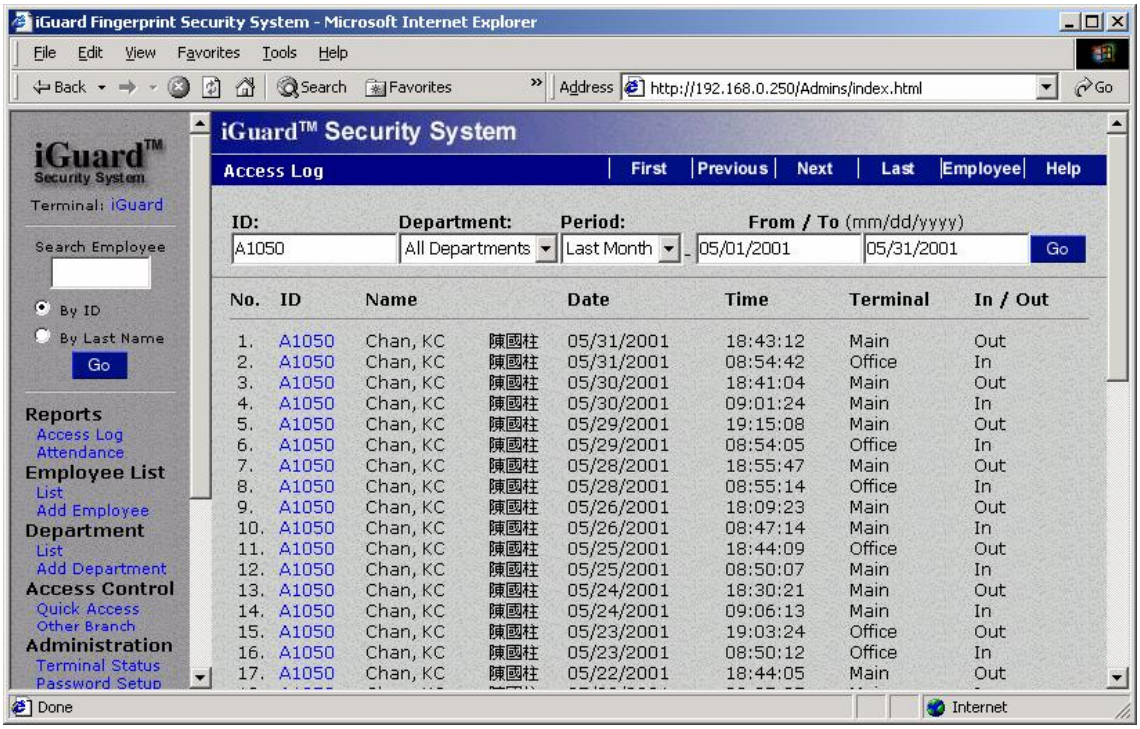
This page shows the employees' Access Records. If you want to show the records of only a particular person (e.g., C001), enter his ID # in the edit box and press the **Go** button, and the browser will only show the records of this person.

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

You can also limit the *Time Period*, such as displaying only Today's records, Last Week records, Last Month records… etc. You can also specify the Time Period by choosing the *Range* selection and entering directly to the From / To fields.

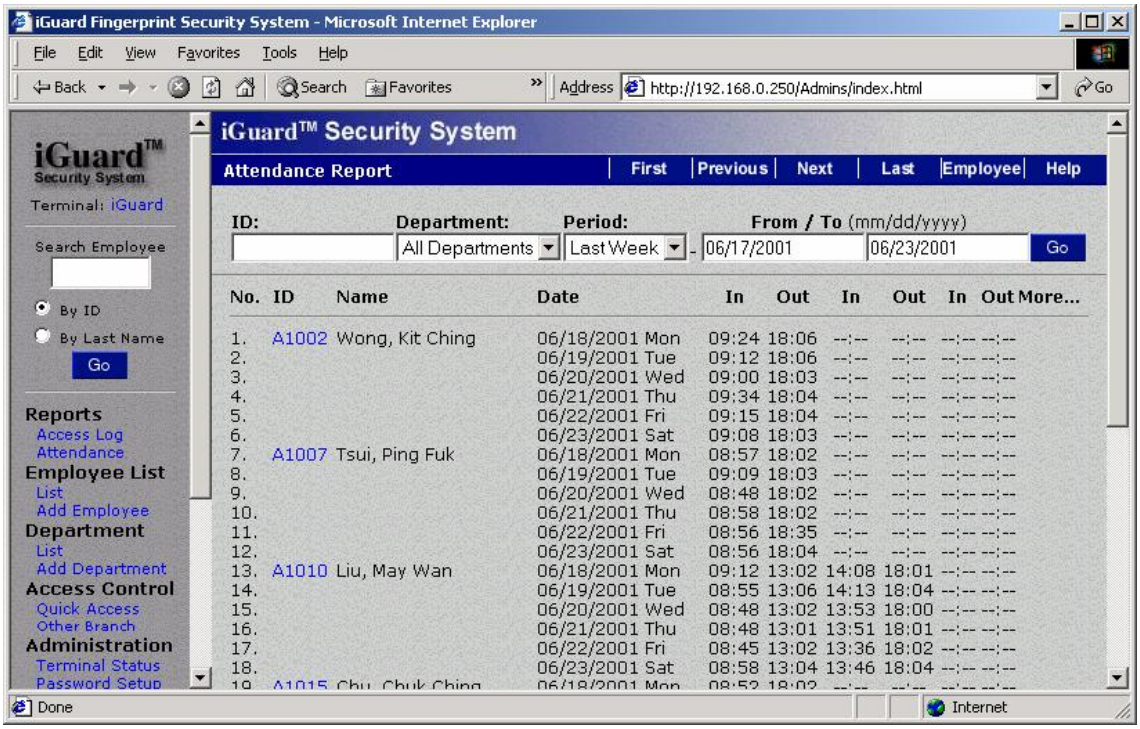
To browser the records, such as to move to next page, press the **Next** button in the navigator bar at the top of the page, or jump to any particular page by clicking on the page number at the bottom.

The following example shows only the Last Month records of the employee ID # A1005: -



Reports – Attendance

The attendance reports provide a consolidated access records of each person as follows: -

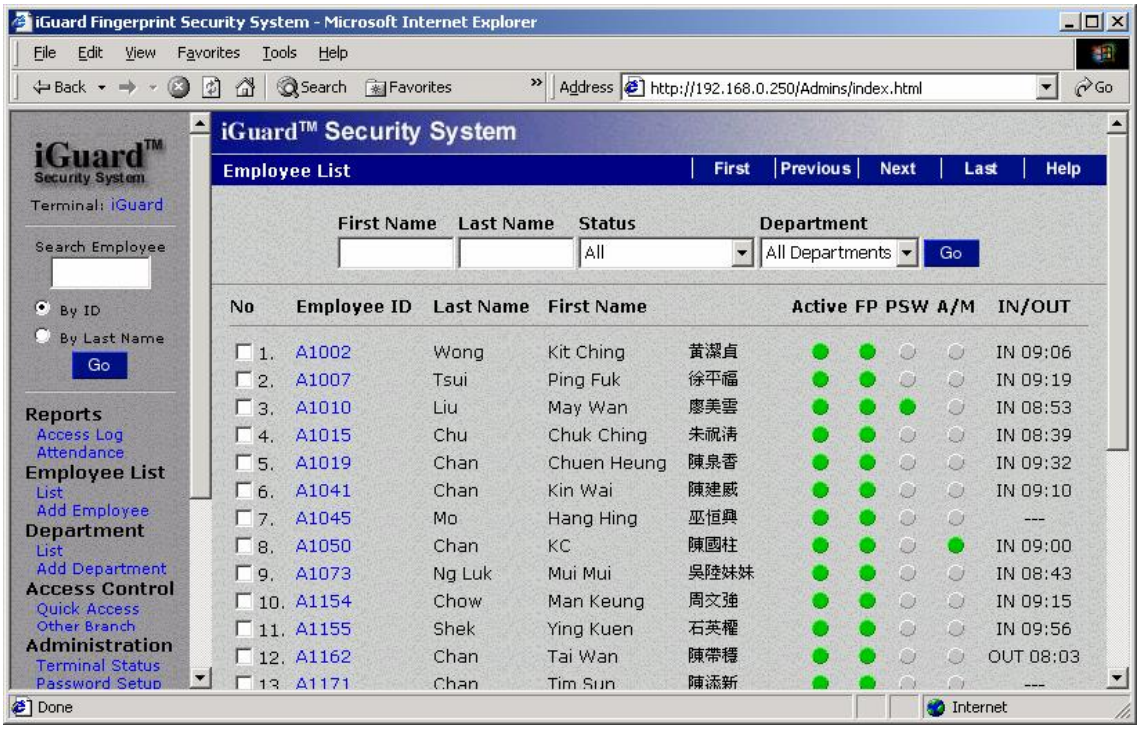


The Attendance Report is particularly useful for payroll purpose. However, it is only meaningful if the system is used as a Time Attendance System. If used as an Access Control System, you can still retrieve the report, but the contents of the report may not be as useful.

Similar to the Access Log Report, you can specify the employee's ID and / or the Time Period of the Attendance Report.

Employee – List

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



There are four *green* indicators listed on the right side of the list:

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

- The ***FP*** (Fingerprint) indicator indicates that the Fingerprint Information is available for the employee. It is possible to add an employee through the browser first, and later on register (enroll) the fingerprint of the employee at the device. If the employee is added this way, the FP indicator will be blank for that employee, until he/she has registered his/her fingerprint image.

- The ***PSW*** (Password) indicator indicates that the user has a personal password. This personal password is used to replace the use of fingerprint to authenticate the person. As mentioned earlier in the manual, there are people with skin problem of their fingers that are unable to work with the fingerprint sensor. These people either have skin problems such as peel-off skin, or have extremely dry

fingers. Once these people are assigned personal passwords, they can use their personal passwords to access the device as follows:

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

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

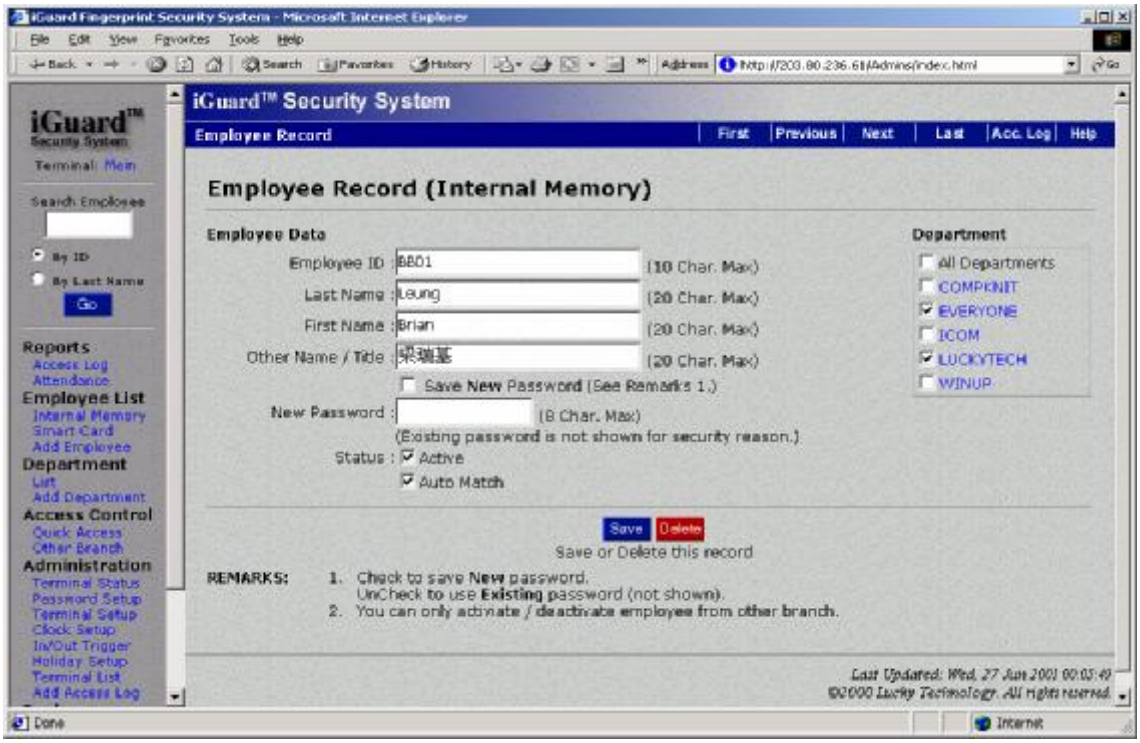
You can also select a group of employees to display in the web page by adding the constraints at the top of the page and press the GO button.

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

Please note that once an employee is deleted, all the data associated with the employee, including the fingerprint information, will be deleted. You must re-enroll the employee again if you decide to add the employee back in the future.

You may be asked to enter the Administrator ID and Password for the operation. The default Administrator ID is "admin", and the default Administrator Password is "123".

You can press the employee ID hyperlink to edit the information of each employee, including the employee's name and the department he/she belongs to, as shown in the following figure.



You can edit the employee information in this page. Press the **Save** button at the bottom to save the change.

You can also delete this particular employee by pressing the **Delete** button.

You can assign this employee to a new department by checking the checkbox of the department on the right side of this page. The default department is EVERYONE. Select the first checkbox, All Departments, to assign the employee to all the departments available. More details about the Department will be discussed in later sections.

A note on the Auto-Match feature: You can assign this feature to any user. Once assigned, the user no longer needs to enter his ID first every time when accessing the device. The user can just simply lift the shutter and place the finger on the sensor. The device will then automatically capture the image of the finger, and will try to match the captured image against the fingerprint information of ALL the auto-matched users. The device will try to match the primary fingers first, and then the secondary fingers. Since it takes about half a second for each matching process, it is recommended to limit the number of auto-matched users to a maximum of ten users.

Employee – Add New

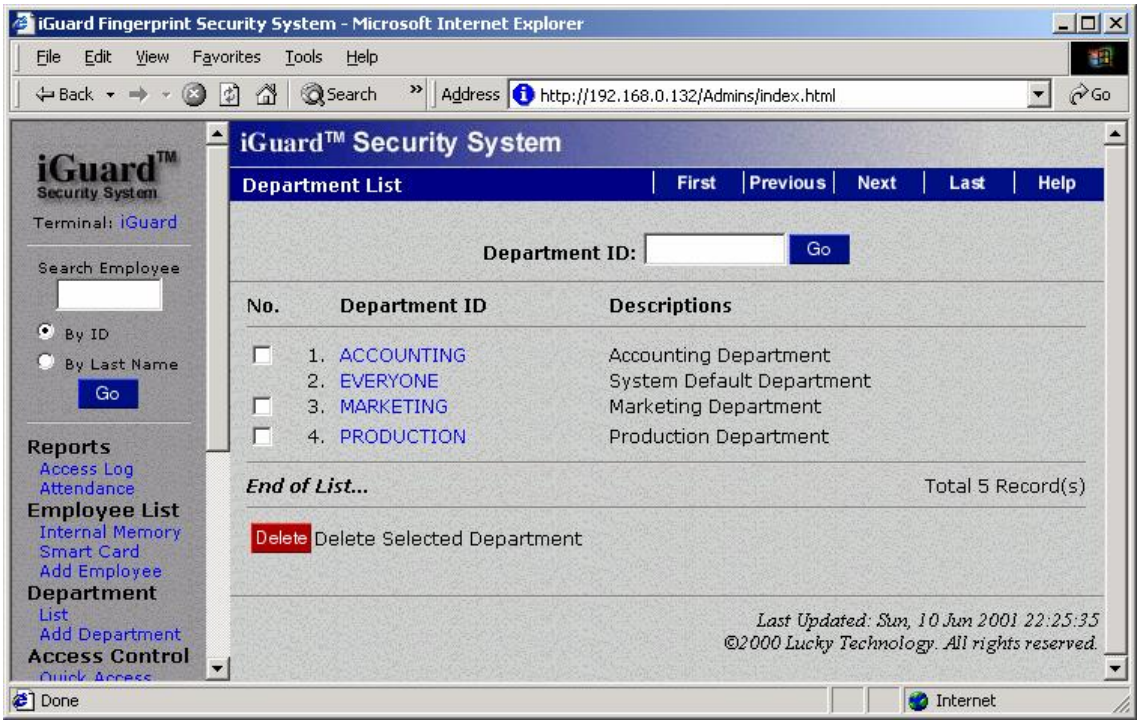
Normally a new employee is added in the enrollment process, as already discussed in the "`Basic Operation – Enrollment`" section. However, you can also add an employee using the *Add New* page. It is basically the same as the page discussed above. Please note that even an employee is added in this page, the

employee is still required to register his/her fingerprint image physically at the device before he/she can authenticate with the device.

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 this time period.

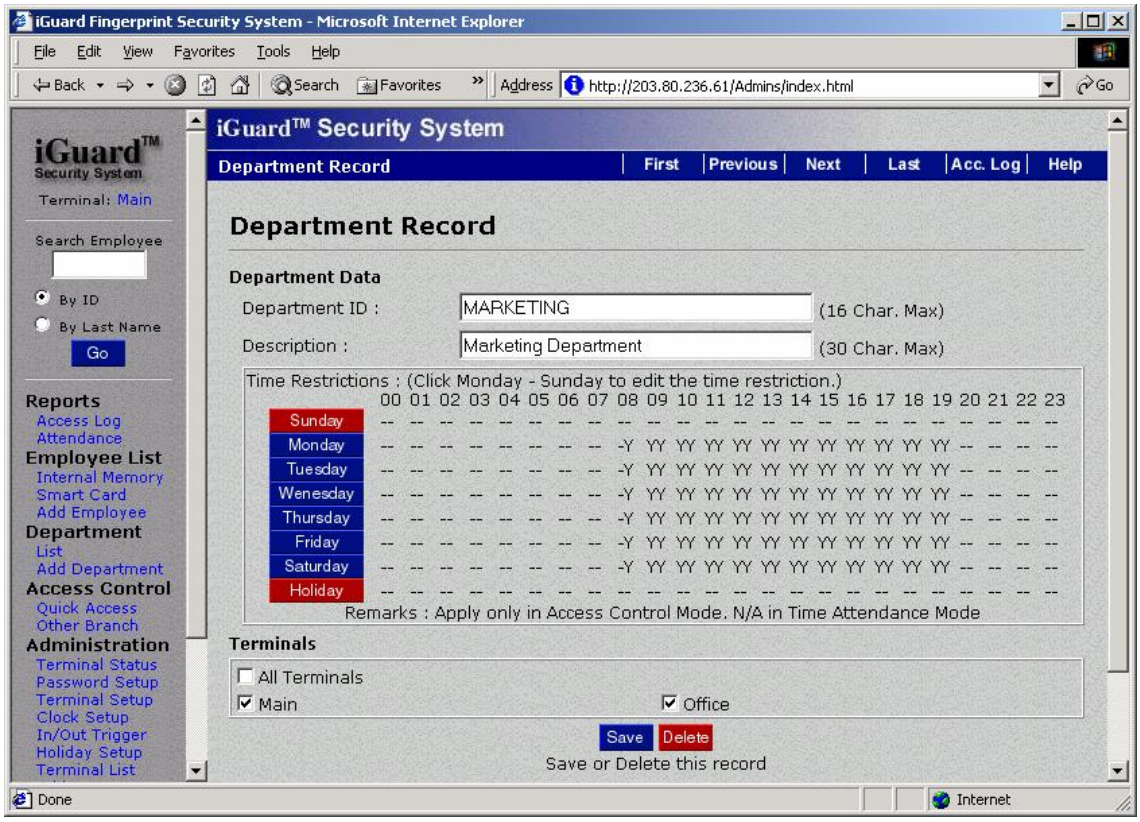
The Department List page is shown as follows: -



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: -

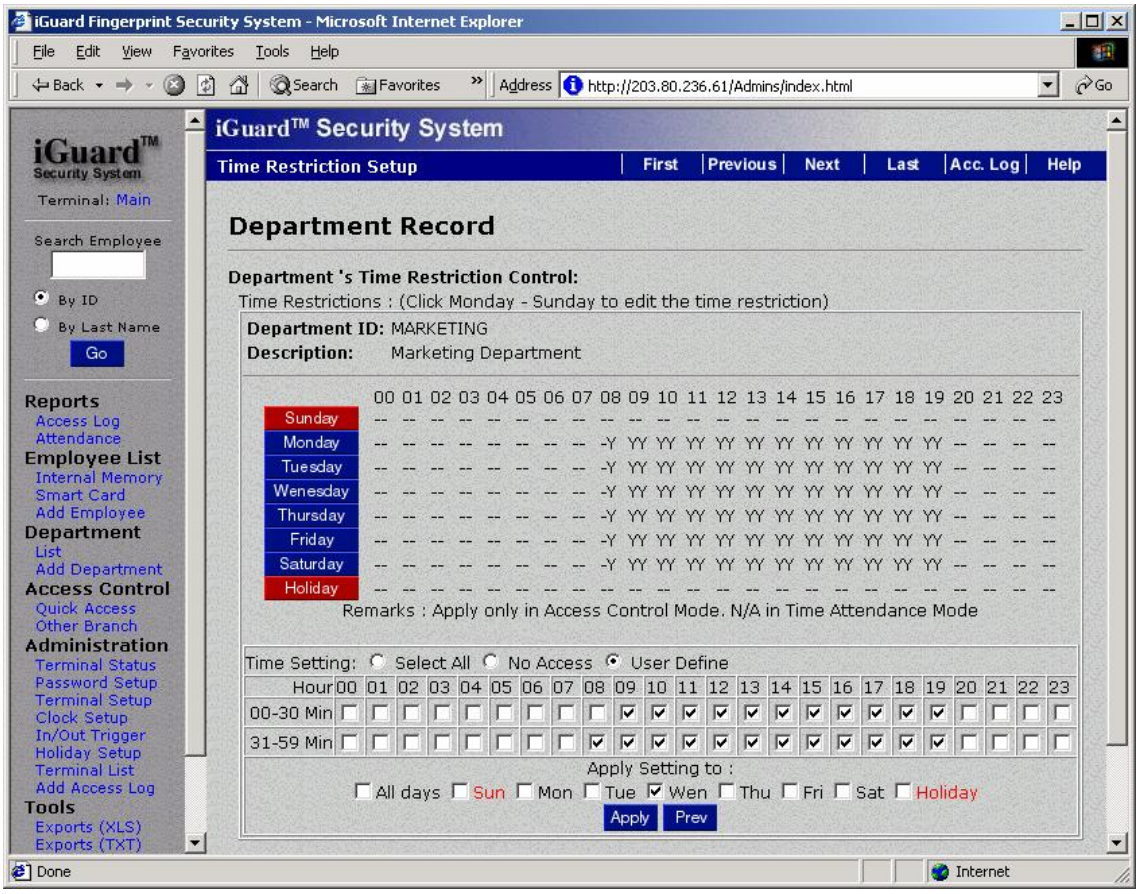


The above page indicates that the authorized time period for the department Marketing is from 8:30 am to 7:59 pm, Monday to Saturday. As a result, all the members of this department can only be authenticated within this period.

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.

The Holiday checkbox will be discussed in later section.

Press the Apply button at the bottom to save the new settings.



Department – Add New

Use this page to add new department. The operation is similar to the steps discussed above.

Access Control – Quick Access

Use this page to define the authorized period in which the Quick Access Password can be used for bypassing the fingerprint authentication process. The default setting is NONE, i.e., you cannot use the Quick Access Password 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 Door Access Password to enter the premises as discussed earlier.

To set up the Door Access Password for Quick Access, please refer to the section **`Administration – Password Setup`** discussed in the next page.

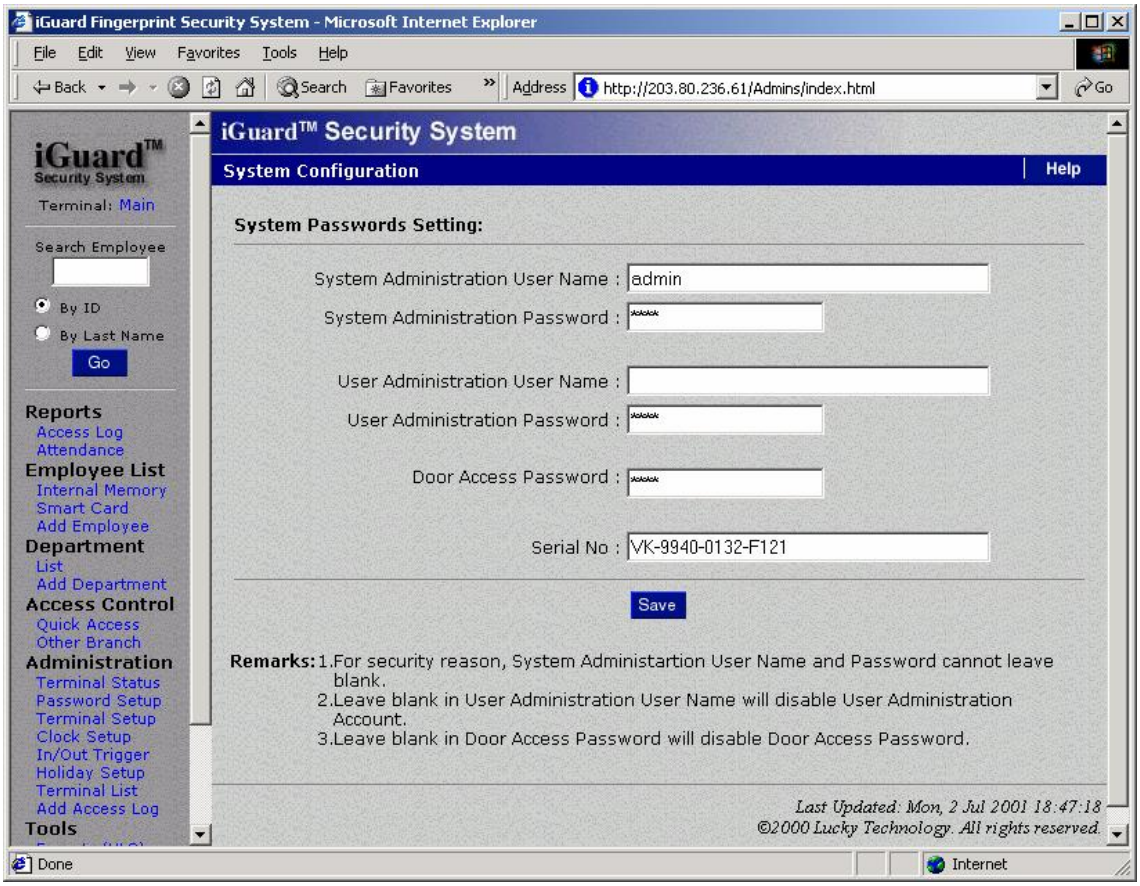
You must set the device to Access Control Mode instead of Time Attendance Mode. To use the Door Access Password to enter the premises, press the **`Func`** key, then enter the Door Access Password (e.g., `123456`), and then press the **`Func`** key again. If the password is correct, and it is within the authorized time, the door will be open.

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.

Administration – Password Setup

Use this page to setup the Administrator Password & the Access Password as follows: -



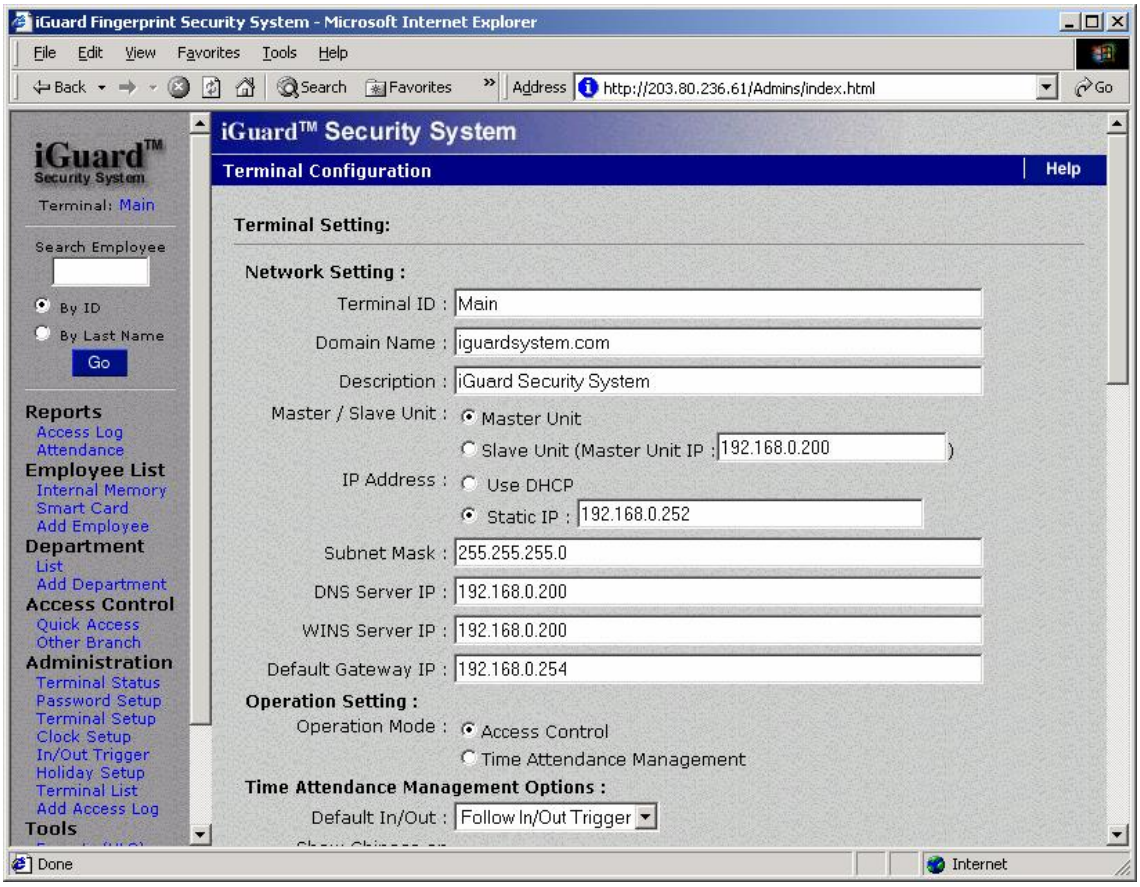
- System Administration – this is the user name and password required to configure the system (such as setting up the IP address of the device), and to administrate the users' settings (such as adding and deleting users). The default name is **`admin`**, and the default password is **`123`**.

- 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.

Administration – Terminal Setup

You can use this page to setup the network configuration of the device as follows: -



Network Setting & Operation Setting

Please refer to the section “Setting the Network / TCP/IP address” on page 12 for explanation of these entries.

Time Attendance Management Options

Default In / Out: This should be set to **`Follow IN/OUT Trigger`**, and the default In / Out status will follow the settings specified in the **`In/Out Trigger`** page. Please refer to the description in *`Administration – In/Out Trigger`* later in this section.

Show Chinese On Terminal: Check the Enable checkbox if you want to show some *pre-defined* Chinese characters in the LCD display of the unit.

Web Server Options

Access Restriction: This is for security purpose in specifying a valid IP address range for accessing the device. Select the "No IP Address Restriction" so any machine from anywhere in the world can access the device. If you want to restrict a specified

range of authorized IP address, select the 2nd choice and enter the range to the box next to it.

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.

Web Page Language: Select the desired language for all the web pages.

Fingerprint Matching Security Level

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, more false rejects of users will be expected.

Door Relay and Beep Setting

Door Relay Control: Normally, in Access Control Mode, the door relay will be closed no matter the user's access status is IN or OUT. If the IN checkbox is disabled, the door relay won't be closed for all the IN accesses. Likewise, if the OUT checkbox is disabled, the door relay won't be closed for all the OUT accesses. This option is useful if the device is installed outside the main door, and the device is used to record the clock-out time of the users. By un-checking the OUT checkbox, the door won't be open if someone clocks out from the device.

Beep Sound: to disable all the beep sounds of the device, if completely quiet operation is required.

Company & Branch Code Settings

These two entries are only useful if your device is equipped with the Smart Card Option.

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 camera is *Axis 2100 Network Camera* from *Axis Communications.*[3] Up to four Web Cameras are supported.

Serial Number

This is the unique serial number of this machine. You may need to provide the information if you need technical support for the device.

[3] http://www.axis.com

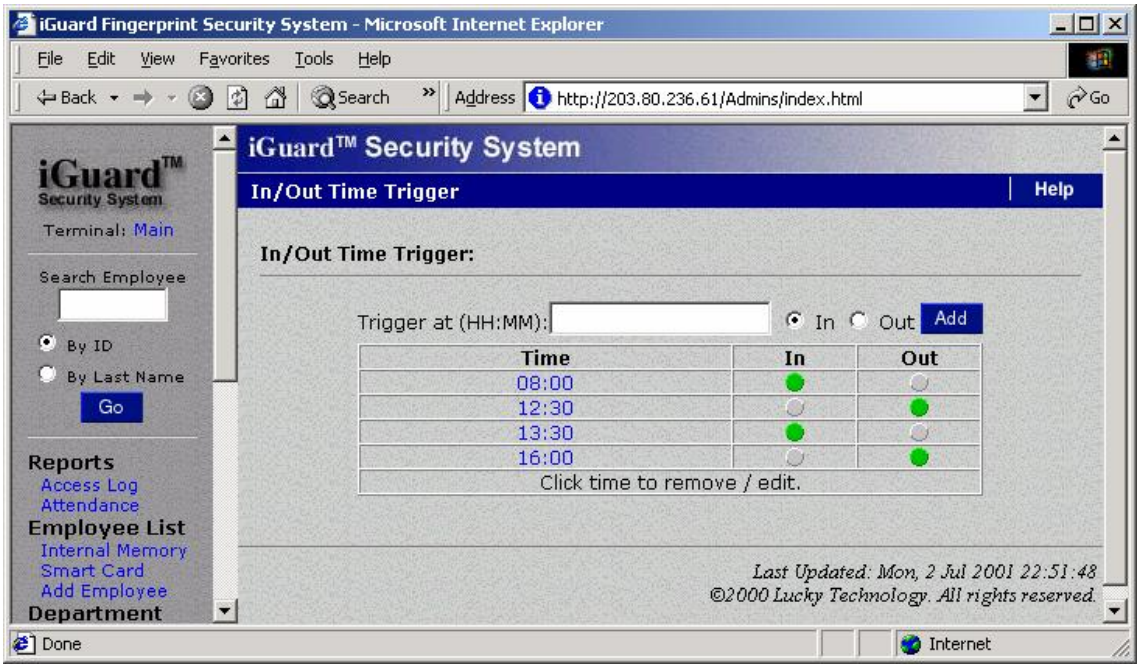
Administration – Clock Setup

Use this page to setup the clock of the device. Please note that if the 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.

There is a software tool to allow you to automatically synchronize the clock with your PC's clock daily. It is available for free download at our website.[4]

Administration – In / Out Trigger

Use this page to setup the In / Out Trigger time for the default In / Out status for Time Attendance Recording.



The In / Out Time Setting is useful only if the device is configured as Time Attendance Mode. 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: -

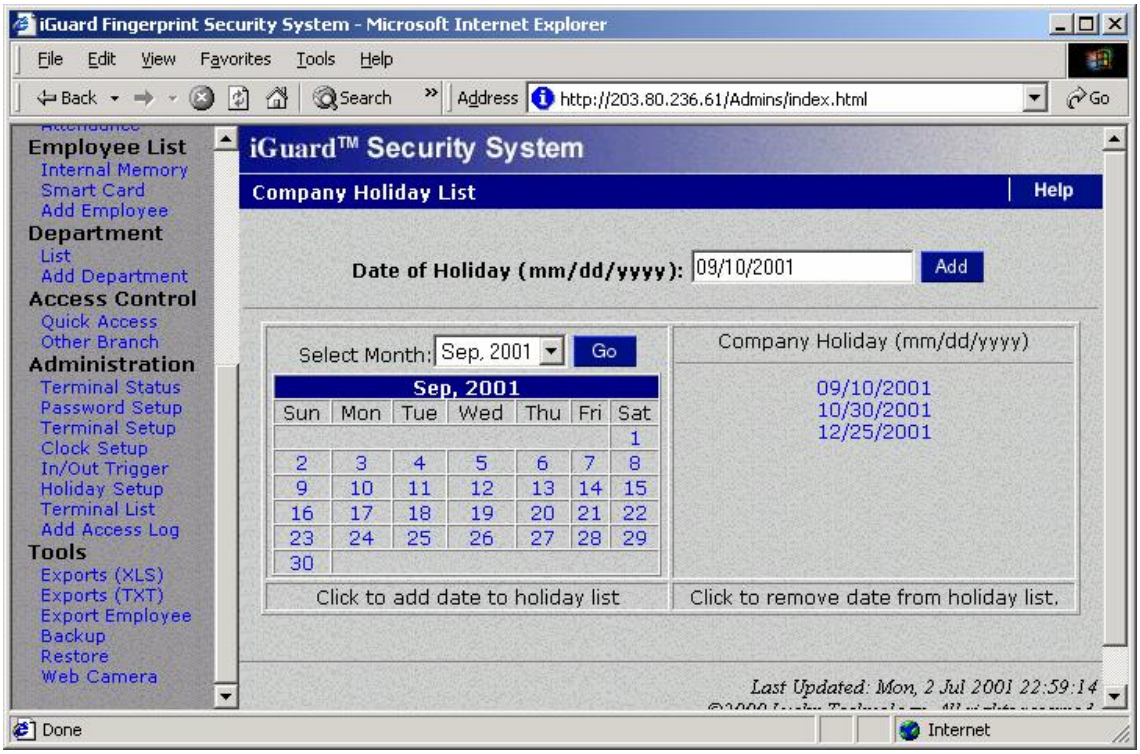
Description	***LCD Display***
1. Default IN (stands for Clocking IN).	`Mon Aug 30 13:49` `ID #:_ IN`
2. Default OUT (stands for Clocking OUT).	`Mon Aug 30 13:49` `ID #:_ OUT`

[4] http://www.iguardsystem.com

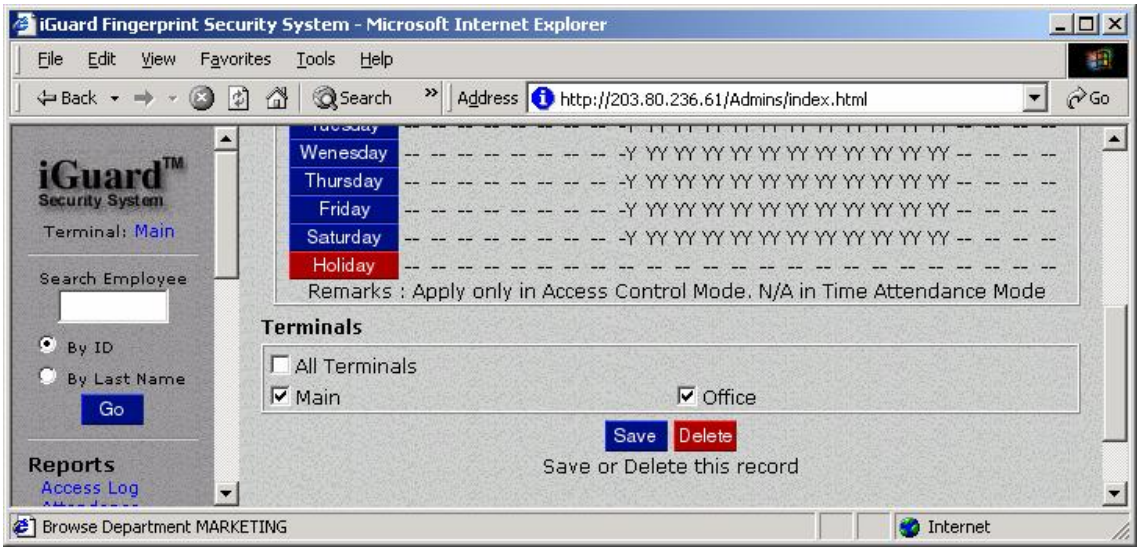
User can override the default setting by pressing the backspace key before entering the user ID.

Administration – Holiday Setup

Use this page to setup the Holiday list. The Holiday list is use for the Time Restriction purpose (along with the day-of-week settings).



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

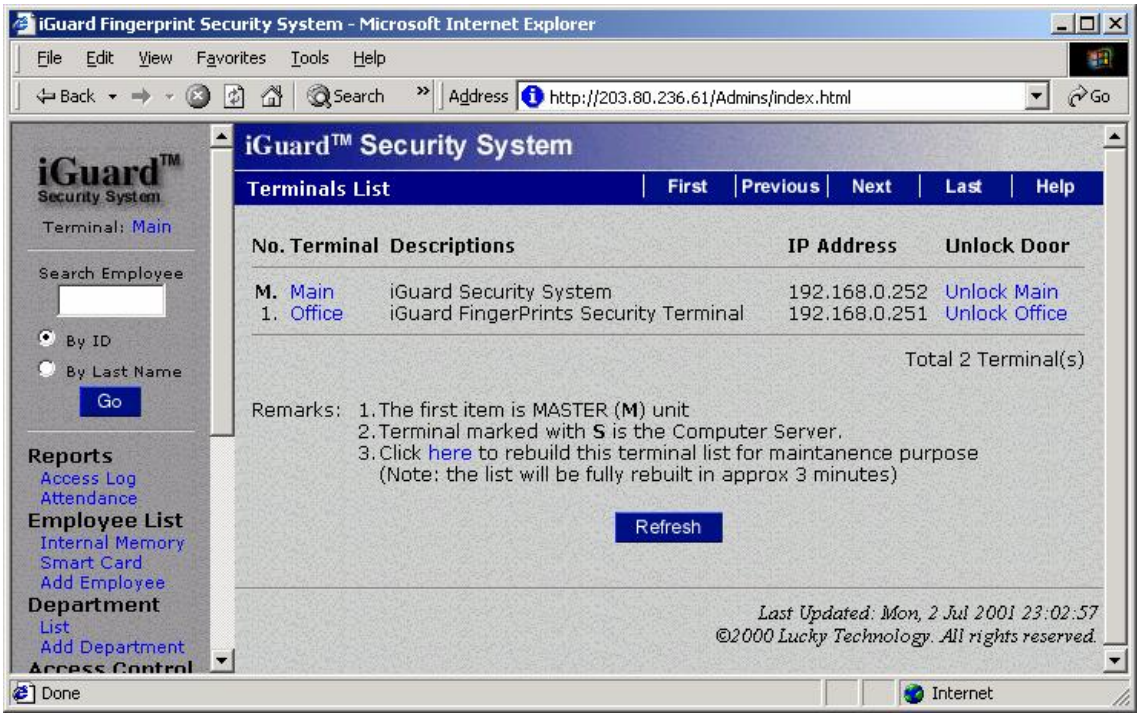


As indicated in the above page, all the employees belong to the Marketing department will not be able to authenticate on the three holidays specified.

Please refer to the section “Department – List” above for how to change the time restriction settings.

Administration – Terminal List

This page shows the current slave devices in the corporate network: -



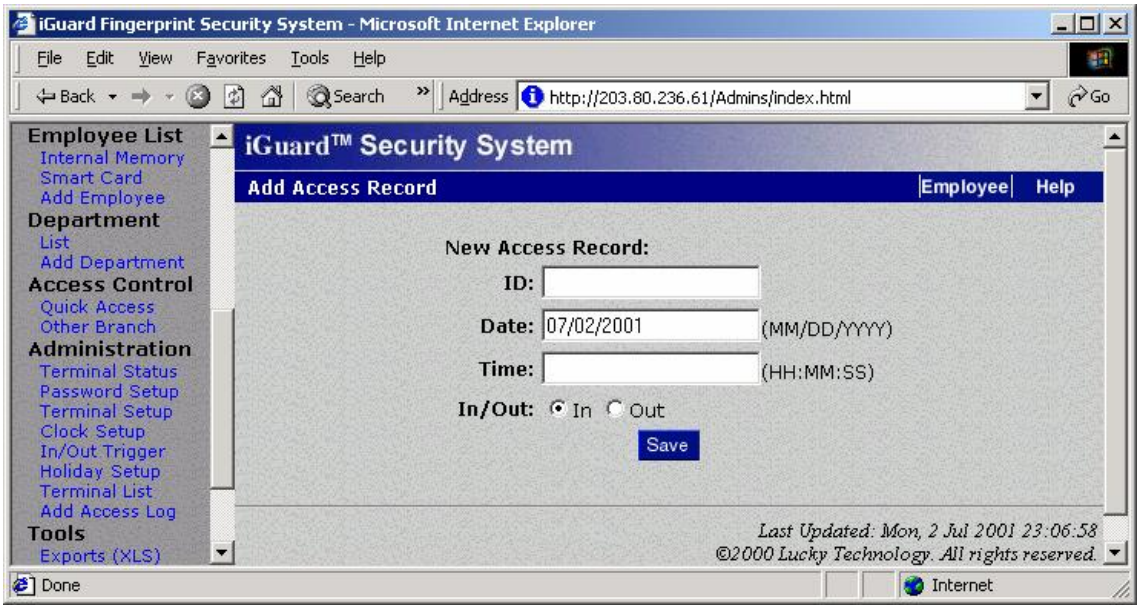
In the above example, the device “Main” is the master unit, and it has one slave unit named “Office”.

The corresponding IP address of each device is also shown.

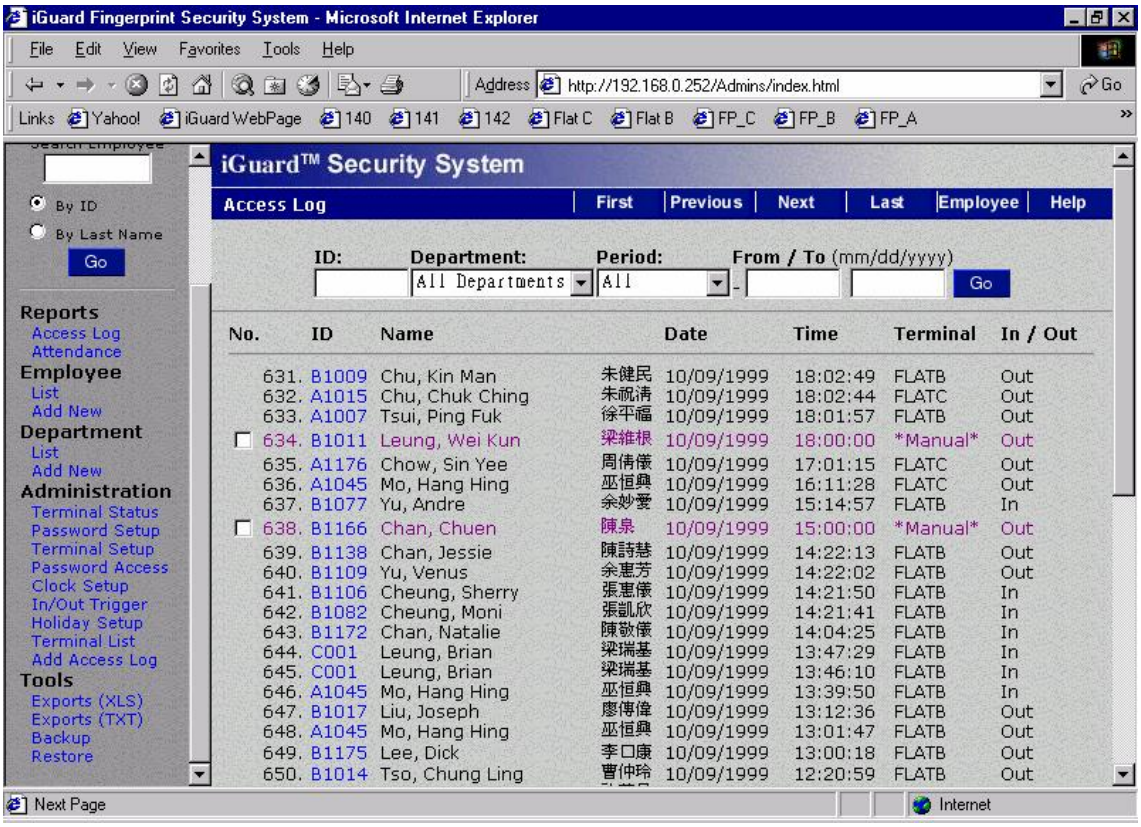
As a convenient feature, you can remotely unlock the doors by clicking the **`Unlock Main`** & the **`Unlock Office`** links.

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 when the device is configured as Time Attendance System.



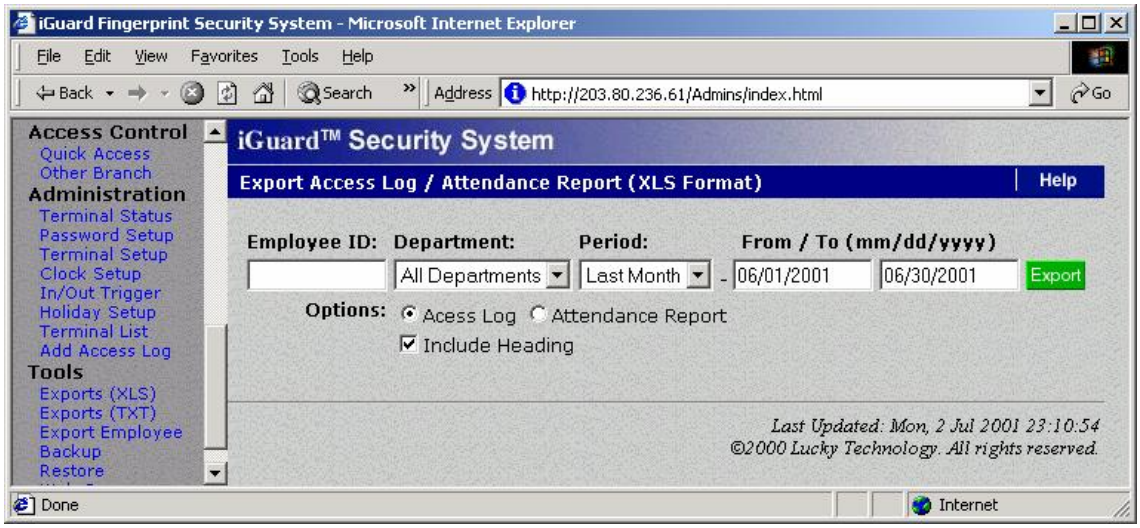
A manually added record is shown differently in the access report as shown below: -



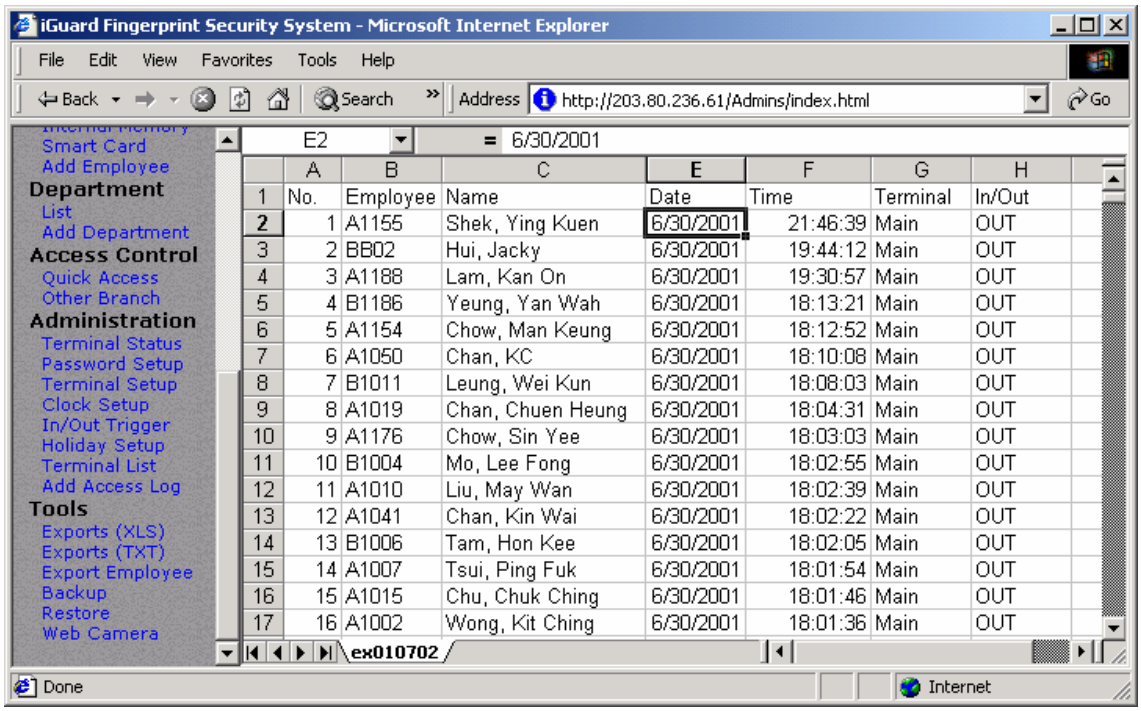
The records in Pink color with the checkbox next to them indicate that these records were added manually. You can later on delete these records by selecting the checkbox and then press the Delete bottom at the bottom of the page.

Tools – Exports (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 (an example can be found in the CD-ROM comes with the device).



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



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:-

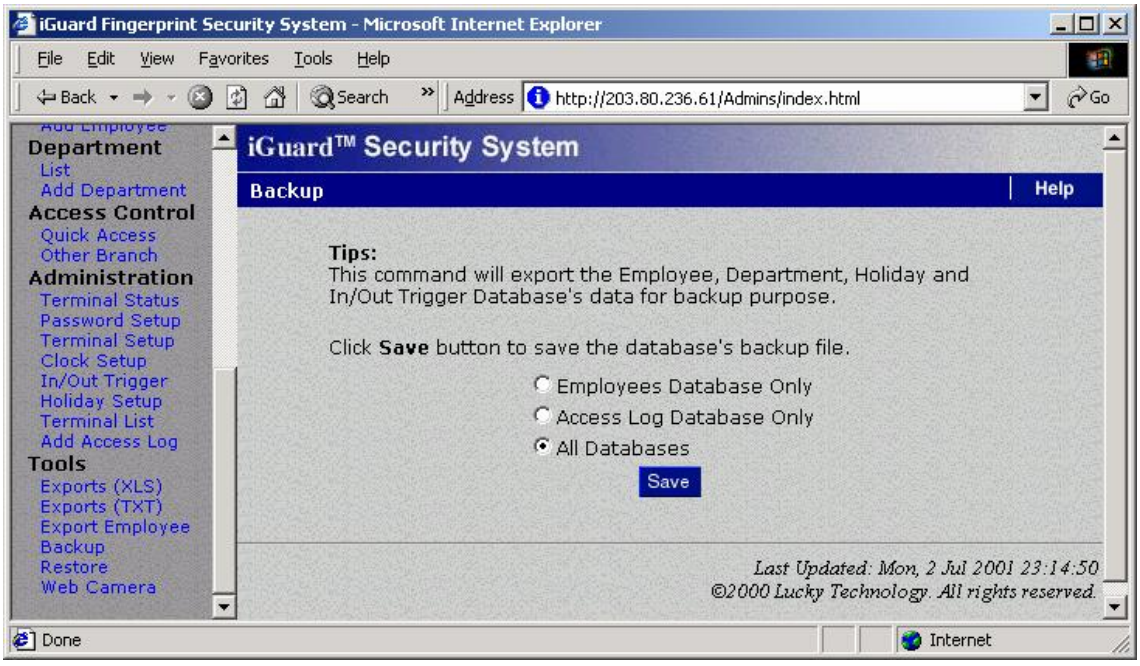
```
"Item","Employee ID","Name","Other Name","Date","Time","Terminal","In/Out"
"1","A1155","Shek, Ying Kuen","admin","09/30/1999","20:02:04","F1103","Out"
"2","B1077","Yu, Andre","account","09/30/1999","19:58:58","FLATB","Out"
"3","C001","Leung, Brian","director","09/30/1999","19:58:50","FLATB","Out"
"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"
```

Tools – Export Employee

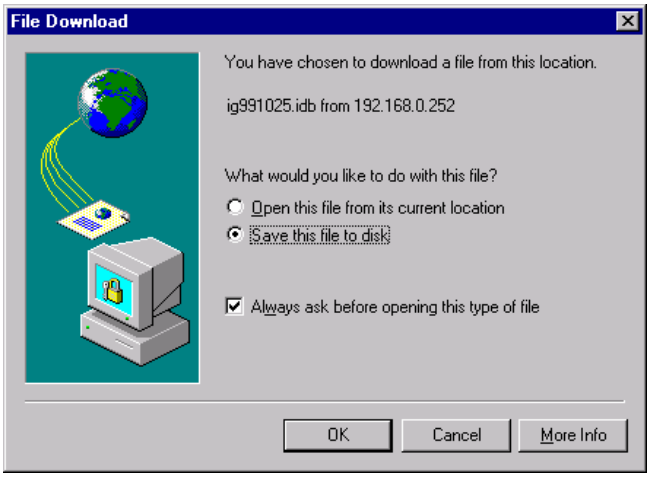
Use this to select and save particular users' information from the user database to another device.

Tools – Backup & Restore

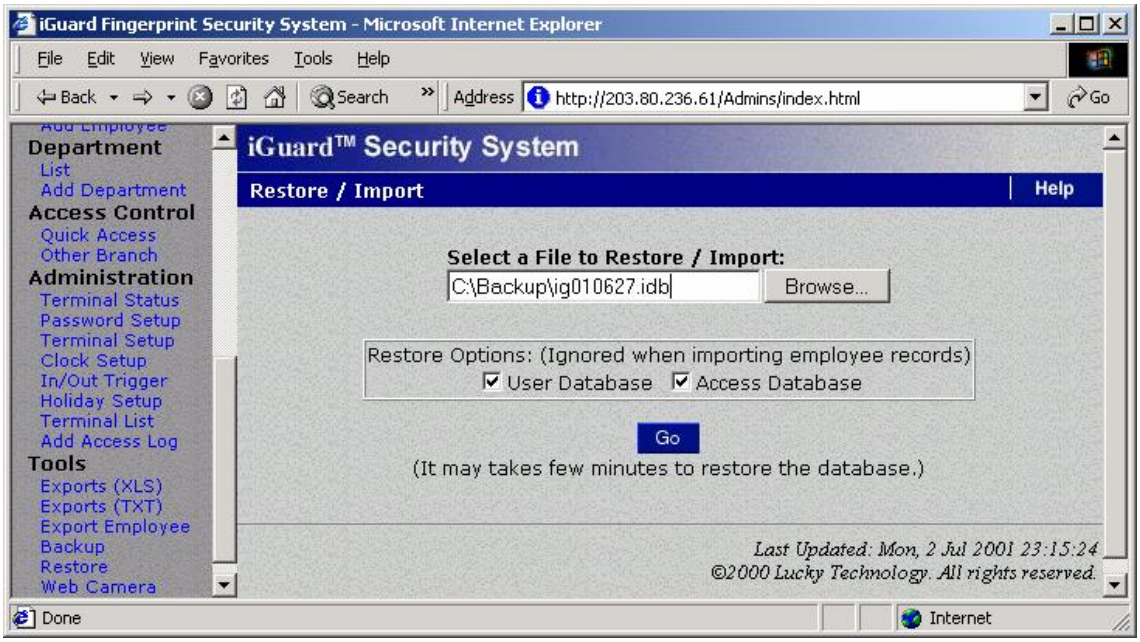
It is suggested to backup the internal data periodically to the desktop computer (such as a daily backup). In the unlikely event that the system is to be replaced, the old data can be restored back to the new device, and the employees do not need to re-enroll again.



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



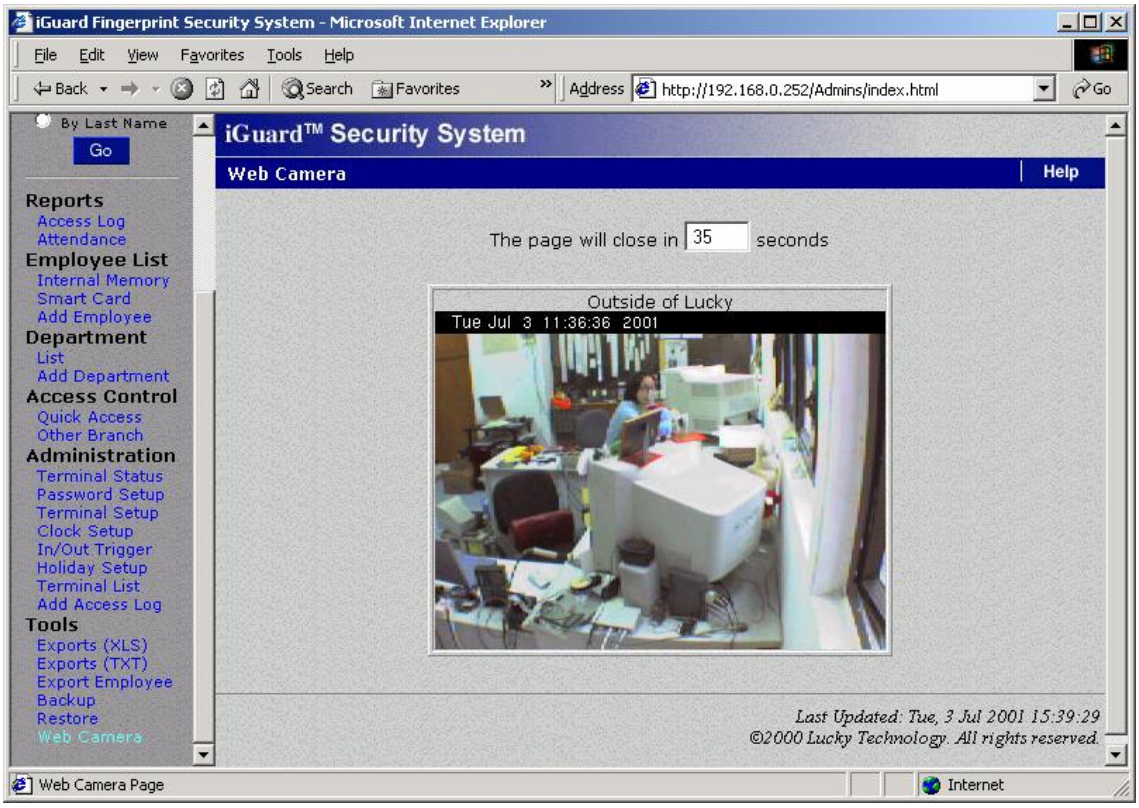
Press the OK button to save the backup data to your desktop computer. When it is necessary to restore the data (for example, a new device has been installed), go to the Restore page and specify the file name as follows: -



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

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: -



Currently the only supported web camera is *Axis 2100 Network Camera* from *Axis Communications.*[5] Up to four Web Cameras are supported at the same time, and can be shown in the same page.

Please refer to the **`Administration – Terminal Setup`** section for more detail in setting up the web cameras.

[5] http://www.axis.com

ADVANCED FEATURES

You can use the built-in advance functions to reset the device to the factory defaults, and to set the device to the *Test Mode* for users to "*practice*" with the device.

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***
1. 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:` `_`
2. Enter the Administrator Password (e.g. 123).	`Enter Password:` `123_`
3. Press the **Func** key, and then select `Function 7` to enter the `System Reset` menu. You will be asked if you want to delete the User Database as shown.	`Reset User DBase` `Yes/No (1/2)? _`
4. Enter **1** if you want to clear all the existing User Information, or else press **2** to keep the existing information. Then you will be asked if you want to delete the Access Database.	`Reset Access Log` `Yes/No (1/2)? _`
5. Again, enter **1** if you want to clear the log, and enter **2** if you want to keep it. You will then be asked if you want to reset the settings to the factory default.	`Factory Default` `Yes/No (1/2)? _`
6. 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`). The system will perform a system reset, and then it will return to `Standby Mode` (it usually takes around 20 seconds).	`Mon Aug 30 12:00` `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 Reset* function to reset all the existing records in the machine.

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 F" in the setup menu to toggle between Test Mode & Normal Mode, and is illustrated in the following steps: -

Description	***LCD Display***
1. 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: _
2. Enter the Administator Password (e.g. 123).	Enter Password: 123_
3. 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 #:_
4. Following the same procedure above and press **"A"** again in the setup menu to put the machine back to Normal Mode.	Mon Aug 30 12:00 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.

THE OPTIONAL SMART CARD

The device can optionally equip with the renowned Philips Mifare Contactless Smart Card Reader.[6] With this option, users can both use the conventional way or the smart card for user authentication. Each user will have his / her own smart card, which stores the user information including the name, company & branch code, and the fingerprint information.

Why need the smart card?

Normally, all the users' information is stored in the internal memory of each device, including the fingerprint template (a mathematical representation of the fingerprint image). The information requires a lot of memory space. Therefore, there is a limitation of the maximum number of users stored, and the current maximum number of users is 1,000.

With the smart card, since the user information is no longer stores in the internal memory, the device can thus support many more users (i.e., up to 5,000 users).

Although it is easy to replicate all the user information across all devices within a Master / Slave configuration, it is not too easy to replicate the data with other branches of the company in different geographic locations. This problem can be solved by using smart card to store the user information, and the user will carry his / her own information with him / her.

Also, this option allows almost-instant verification during the authorized period for entry, thus enables high-traffic applications (such as during the beginning of the day when everyone gets to the office at about the same time).

Internal Memory vs. Smart Card Memory

The internal user database of the device is divided into two parts: the ***Internal Memory*** & the ***Smart Card Memory***. The Internal Memory acts as both the *temporary storage* to store the user information (for transferring to the smart card later), and as the *permanent storage* for the auto-match purpose. The maximum number of users stored in the Internal Memory is 20.

The Smart Card Memory stores the information of the smart cards that have been registered to the device. The information includes the serial number of the card, the user name, the departments the user belongs to, the access rights of the user, but *without* the fingerprint information. The maximum number of smart card users stored in the Smart Card Memory is up to 5,000.

[6] MIFARE® is an interface platform for contactless smart cards and readers according to the ISO 14443 A Standard. Please refer to http://www-us.semiconductors.com/identification/products/mifare/ for more details.

The Company Code and the Branch Code

Two new codes, the *Company Code* and the *Branch Code*, are 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.

On the other hand, the Branch Code is to identify different branches of the same company. Each branch should have its own unique branch code. For example, the Branch Code of the Hong Kong Branch can be assigned as `HKG`, and the one for the USA branch can be assigned as `USA`.

The purpose of the branch code is to uniquely identify a person. For example, there may be a user with a user ID `A123` in branch `HKG`, and there is another user in branch `USA` with the same ID, and they are differentiated by this branch code.

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

Basic Operation

Similar to the basic model, all the users must enroll in the device first. The enrollment procedure is identical to the one in the basic model (i.e., via the *Function 1* in the Setup Menu described in page 16). After the enrollment procedure, the user ID and the fingerprint template is stored in the Internal Memory.

You can modify the user information, such as the user name, via the web browser as in the basic model. You can also assign the departments that the user belongs to. The Internal Memory page is similar to the Employee List page described in previous sections.

Also, similar to the basic model, users can authenticate by entering his user ID and then present his finger to the sensor. The Auto-Match feature is also available to these users too.

Once the user information is stored in the Internal Memory, you can *write* the information from the Internal Memory to the user's Smart Card (via **`Function 9`** of the Setup Menu). During the write procedure, all the user information, including the fingerprint template, is written to the smart card. And at the same time, an extra copy of the user information is created in the Smart Card Memory. The information includes the User ID, user name, user's personal password…. etc., except the fingerprint template. In addition, the serial number of the smart card is also included.

After writing to the smart card, you have an option whether to delete the user information from the Internal Memory or not. In most cases you should delete the

user information from the Internal Memory. It is because the Internal Memory is only used to temporarily store the user information, and the maximum number of users stored in the Internal Memory is only 20. However, if you want the user to have the auto-match feature, you must not delete it from the Internal Memory.

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

Description	***LCD Display***
1. 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 **9** to select "`Write SmartCard`" menu.	`Enter ID :` `_`
2. Enter the ID # you want to write to the Smart Card (e.g., A01).	`Enter ID :` `A01_`
3. Press the **Func** key to confirm. You will then be asked to present the Smart Card.	`Waiting for` `Smart Card...`
4. Present a Smart Card near the keypad. The unit will then write the user information to the card.	`Writing....`
5. After writing to the card, you will be asked whether or not to delete the user from the Internal Memory.	`Del Internal Mem` `Yes/No (1/2)? _`
6. Press **1** to delete the user from the Internal Memory, and 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.

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

Description	***LCD Display***
1. While in Standby Mode, present the smart card near the keypad. The unit will read the data stored in the card, 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..`

2. If 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!`
	:
	:
	`Mon Aug 30 12:00`
	`ID #:_`

Registering an existing Smart Card (Function 0)

The first time a user accesses a remote unit in a remote branch with his 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 card to access the remote unit same as the one in his 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***
1. 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 **0** to select "`Add New SmartCard`" menu. You will then be asked to present the smart card.	`Waiting for SmartCard....`
2. Place the smart card near the keypad, and the unit will read the card and register the card to the Smart Card Memory. The unit is now ready for the next card.	`A01 Registered!` **:** `Waiting for SmartCard....`
3. Press the **BackSpace** key to return to Standby Mode.	`Mon Aug 30 12:00 ID #:_`

You can delete a registered smart card later via the web browser, and it is discussed in the following section.

If it is the authorized time for the *Quick Access* (discussed in page 29), and the unit is also the authorized unit, the Smart Card user can just simply present his card and get authorized, without the need to present his fingerprint for fingerprint matching. This is especially useful during the high traffic period, such as during the start of the day when everyone needs to access the device at the same time.

The Smart Card Memory Page

The Smart Card Memory page is shown as follows: -

The page is very similar to the Internal Memory one, except that it has one additional column (i.e., the *Branch* column), and has only one *Active* Indictor.

You must assign the departments each smart card user belongs to by clicking on the user ID. You will see the web page similar to the following one: -

Select all the departments the user belongs to, and click the **Save** button to save the new settings.

Please note that the Auto-Match feature is not available for Smart Card users. It is because the fingerprint information of the smart card users is not stored in the Internal Memory; therefore it is unable to have this feature for Smart Card users.

--- END ---