AVI INFOSYS L.L.C
DEFINE ▸ DESIGN ▸ DEPLOY

iGuard®

FINGERPRINT/ CONTACTLESS SMART CARD ACCESS CONTROL & TIME ATTENDANCE SYSTEM

International Operations:

AN ISO 9001:2008 CERTIFIED
IT SOLUTIONS PROVIDER COMPANY

FQC
FIRST QUALITY CERTIFICATION
ISO 9001:2008

Deutscher Akkreditierungs Rat
DAR

www.iGuard.me

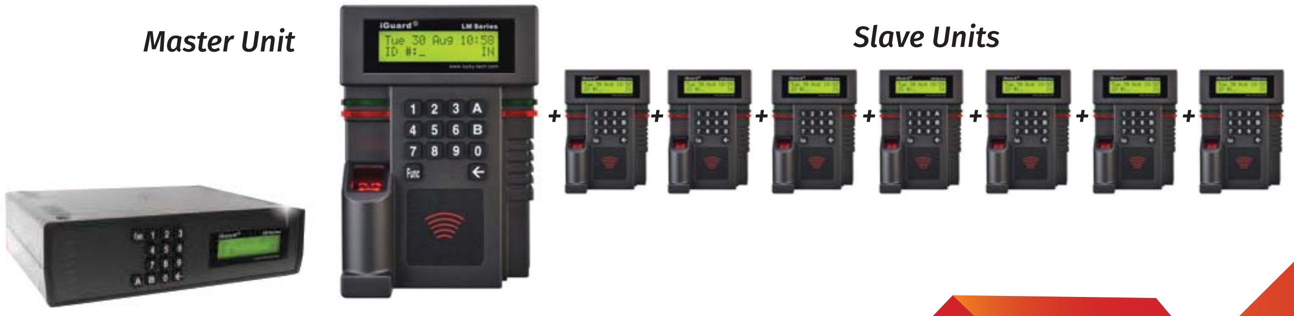
SEE THE WEB SERVER IN ACTION

Each iGuard Biometric/Smart Card Security Appliance has a built-in Web Server enables all the computers in the corporate network to directly simultaneously access the device using any Internet Browser, such as Microsoft Internet Explorer Netscape Navigator. Different computer plat-forms such as Apple Macintosh, Microsoft Windows Linux machines can access the device. No additional software is required. So whether you are in an airport lounge or a hotel room, you can always check if your employees are already in the office or not, and you can even control, modify or disable their access rights to your office remotely via intenet connection provided your iGuard Biometric/ Smart Card Security Appliance is connected to an external IP address or your network is available through a VPN connection that is reachable from your location.

> *With iGuard, users can be authenticated and verified through either Fingerprint, Smartcard or Password. And depending on the different time period, you can set up the iGuard that the users can just simply presents his smartcard to get authorized (such as during high-traffic period), or requires the high-security fingerprint verification (such as after office hours or during weekends and holidays).*

When you can easily and conveniently assign different access rights to your employees. you can plan your security better and maximize the effectiveness of the human resources. And with the built-in Web Server technology, iGuard empowers you to manage the access rights of each individual employees or a group of employees easily anytime, anywhere using any web-enabled computers or mobile devices. For example, you can assign the staff members of the marketing department the rights to get in the office premises during weekdays from nine to five only, or prevent a particular employee from entering the computer server room. Reports: iGuard includes three built-in reports: Access Log, Attendance Report & Daily In/Out report, that can be accessed via any web-enabled computer with web browser. Should more sophisticated reports be required, such as for the payroll purposes, the information can be downloaded and saved in Microsoft Excel format and in plain text format. In addition, the access records can be saved in any PC in the network in the popular ODBC database format in real-time manner, and other applications can conveniently obtain the information from the ODBC (the required software, iServer is available free-of-charge in our download page)

Network up to 255 Total Devices Across a Single Domain



HOW IT WORKS AS AN ACCESS CONTROL SYSTEM

iGuard analyzes & compares a persons fingerprint against the previously enrolled record. If the two fingerprints match, the person is authenticated. And if the time is within the authorized period for entry, the device will signal release the electric door lock.

STEP 1
Enter
Employee ID

STEP 2
Place the thumb on
the door sensor

STEP 3
The door is unlocked
if authenticated

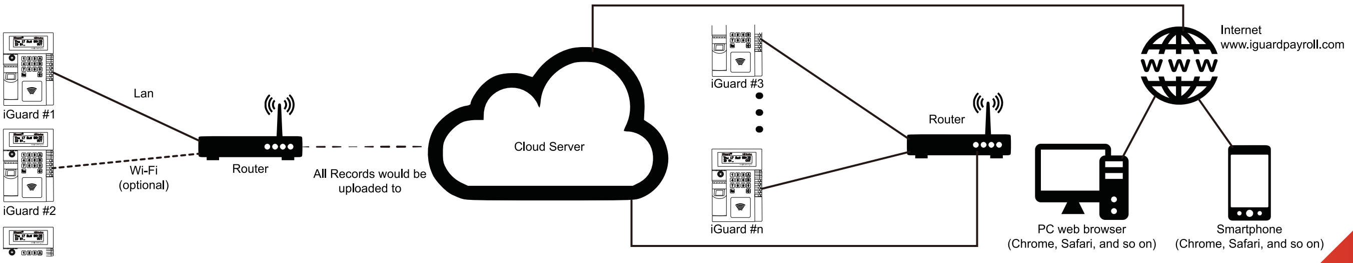
The iGuard Security System analyzes and compares a persons fingerprint against the previously enrolled record. If the two fingerprints match, the person is authenticated. And if the time is within the authorized period for entry. the device will signal and release the electric door lock.

- **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.
- **Password/Fingerprint Access** - you can define the period in which password ran 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.

The Access Control Mode controls the employees from entering the business premises. The system controls the electronic door strike to lock / unlock the door. Users can be assigned to different departments and the authorized time for members in each department can also be controlled. In a multi-device environment, the access rights for each department in accessing different terminals can also be assigned.

HOW IT WORKS - AS A TIME ATTENDANCE SYSTEM

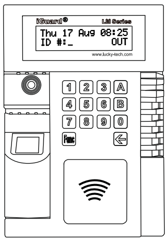
When configured as a Time Attendance System, a user can specify whether he/she is clocking-in or clocking-out By using fingerprints to determine identity, buddy-punching problems can be totally eliminated as well as other fraud. Attendance of each employee is printed on the attendance report. The attendance report is particularly useful for payroll purposes. Wages and salaries can be paid according to the employees worked hours, overtime etc. Wages and salaries can be integrated with a smart card or automatic deposit payroll system.



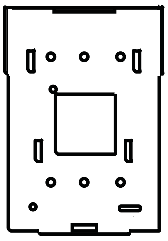
TECHNICAL SPECIFICATIONS

Fingerprint Sensor Type	Optical
Card Reader Type	Contactless Smart Card Reader
	Mifare 14443A
No. of Users	1,000
No. of Access Log Records	20,000
Input Power	12V DC, 700mA
Dimension	105(W) x 40(D) x 150(H)
False Rejection Rate	< 1%
False Acceptance Rate	< 0.01%
Network Interface	Ethernet (100Base-T)
	Wifi (optional)
External Controls	Door Strike, Open-Door Switch, Break-in Alarm, Door Status
Data Output	TCP/IP, Wiegand
Optional Accessories	Remote door relay, Power adaptor

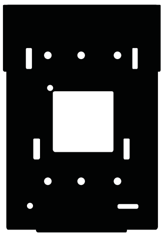
WHAT'S IN THE BOX



iGuard



Metal Plate



Mounting Pad

Hexagonal Screw

Hex Key

Head Office:

P.O Box 26813, Suite 304, Office Court Building, Oud Metha, Dubai, United Arab Emirates

☎ +971 4 358 7036

✉ info@avi-infosys.com

Toll Free 800 AVI (800 284)

www.avi-infosys.com

24 Hours +971 4 3587036