

# ACTAtek3 Manual

Version 1.6  
November, 2013  
ACTAtek Pte Ltd

## Revision History

<b>Revision</b>	<b>Date</b>	<b>Description</b>	<b>Author</b>
1.0	2010/03/29	Initial Release	Cheong / Justin
1.1	2011/05/18	Updated chapter 2, chapter 8	Cheong
1.2	2011/11/21	-Correct RS232 back panel ports diagram -Update Thailand Office contact info	Peter
1.3	2013/08/02	-Add/Update new ACTA3 features	Peter
1.4	2013/08/15	-Add Emergency mode feature -Additional Security Options	Peter
1.5	2013/08/23	-Add JP19 Wiegand Output/RS485	Peter
1.6	2013/11/07	-Add Door Switch/Door Sense -Audit Log function -New LCD display -Web enrollment for FP/SC users	Peter

## **ACTAtek3 Manual**

Copyright 2004 – 2013 ACTAtek Pte Limited, All rights reserved.

No part of this document may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language, in any form or by any means, electronic, mechanical, magnetic, optical, chemical, manual or otherwise without the prior written permission of ACTAtek Pte Limited.

ACTAtek is a registered trademark of ACTAtek Pte Limited

All trademarks, registered trademarks, and service marks are the property of their respective owners.

## Offices:

### **Asia and the Rest of the World:**

Unit 901-2, 9/F, Fo Tan Industrial Centre,  
26-28 Au Pui Wan Street,  
Fotan, Shatin, Hong Kong.

Tel: 852 2319 1333  
Fax: 852 2776 8997  
Email: [sales-row@actatek.com](mailto:sales-row@actatek.com)

### **Americas (North and South America):**

ACTAtek Technologies Inc.  
Suite 230, 10691 Shellbridge Way  
Richmond, BC V6X 2W8  
Canada

Phone: 604 278 8888  
Fax: 604 278 6082  
E-mail: [sales-ca@actatek.com](mailto:sales-ca@actatek.com) (Sales Enquiries)

### **Europe, Middle East & Africa:**

ACTAtek (UK) Ltd.  
Unit 7 Lightning way,  
West Heath, Birmingham B31 3PH  
U.K.

Phone: 44 121 411 2288  
Fax: 44 121 411 2299  
Sales Tel: 44 121 288 9923  
E-mail: [sales-EU@actatek.com](mailto:sales-EU@actatek.com) (Sales Enquiries)

### **Singapore & Malaysia:**

ACTAtek Pte Ltd  
18, Boon Lay Way, #09-96/97/98  
Tradehub 21, 609966  
Singapore

Phone: 65 65154520  
Fax: 65 65154521  
E-mail: [Sales-asean@actatek.com](mailto:Sales-asean@actatek.com) (Sales Enquiries)

### **ACTATEK (THAILAND) CO. LTD.**

378 Soi Laphrao 101 Yaek Soi 12 Laphrao Road Klong Jan Bangkok 10240  
Tel/Fax: 66 3781072 Mobile: 66 917381808  
E-mail: [Sales-asean@actatek.com](mailto:Sales-asean@actatek.com) (Sales Enquiries)

## Table of Contents

Chapter 1. Introduction.....	8
1.1. Purpose .....	8
1.2. Document Conventions.....	8
1.3. Intended Audience and Reading Suggestion .....	8
1.4. Software References for this document .....	8
Chapter 2. Product Overview .....	9
2.1. ACTAtek3 Model number.....	9
2.1.1. Legend .....	9
2.1.2. EXAMPLE .....	9
2.2. Comparison between Fingerprint and Smart Card Models:.....	10
2.3. Warranty:.....	10
2.4. Setup Requirements .....	12
2.4.1. Operating System (For access via Corporate Network).....	12
2.4.2. Network Interface .....	12
2.4.3. Power Requirements .....	12
Chapter 3. ACTA3 Structure and Connections.....	13
3.1. ACTAtek3™ Internal Structure and Connections .....	13
3.2. Connection Details:.....	15
3.2.1. JP18.....	15
3.2.2. JP20.....	15
3.2.3. J3 .....	15
3.2.4. J4 .....	15
3.2.5. JP17 .....	15
3.2.6. JP19.....	15
3.2.7. J6 .....	15
3.2.8. P4.....	15
3.2.9. J2 .....	15
Chapter 4. FingerPrint Notes .....	16
4.1. Introduction .....	16
4.2. Technical Information.....	16
4.3. Good Image vs Bad Image .....	17
4.4. Fingerprint Enrollment & Authentication .....	18
4.5. Fingerprint Enrollment:.....	19
Chapter 5. ACTAtek3 Introduction .....	20
5.1. Introduction .....	20
5.2. LCD Module .....	21
5.3. Keypad Module .....	21
5.4. Fingerprint Scanner Module .....	22
Chapter 6. System Configuration .....	23
6.1. Login.....	23

6.2.	Add User.....	25
6.2.1.	Adding A New User via Fingerprint.....	25
6.2.2.	Adding A New User via Smart Card.....	26
6.2.3.	Deleting A Smart card user .....	27
6.2.4.	Adding A New User via Password .....	28
6.3.	Error Messages.....	29
6.4.	User Management .....	31
6.4.1.	User Management – Activating A User.....	31
6.4.2.	User Management – Deactivating A User.....	31
6.4.3.	User Management – Deleting A User .....	32
6.5.	Auto Match.....	33
6.5.1.	To Enable Auto Match .....	33
6.5.2.	To Disable Auto Match .....	34
6.6.	Date & Time.....	35
6.6.1.	To Modify the Date Settings .....	35
6.6.2.	To Modify the Time Settings.....	36
6.7.	IP Settings .....	36
6.7.1.	IP Address Configuration.....	37
6.7.2.	Default Gateway Configuration.....	37
6.7.3.	DNS IP Configuration .....	38
6.7.4.	Subnet Mask Configuration .....	38
6.7.5.	DHCP IP Configuration.....	39
6.7.5.1.	To Enable DHCP:.....	39
6.7.5.2.	To Disable DHCP:.....	39
6.8.	Terminal Settings.....	40
6.8.1.	Terminal Settings Function.....	40
6.8.1.1.	Fingerprint Security Level Settings .....	40
6.8.2.	No. of FP Sample .....	41
6.8.3.	Unlock Door .....	41
6.8.4.	System Reboot.....	42
6.9.	Reset .....	42
6.9.1.	Resetting the Event Log .....	43
6.9.2.	Resetting the User Database .....	43
6.9.3.	Factory Default .....	44
6.9.4.	Web Port .....	44
6.10.	Exit.....	44
Chapter 7.	Web Administration .....	45
7.1.	SSL Certification – Data Encryption .....	46
7.2.	Terminal Status.....	47
Chapter 8.	Super Administration Guide.....	48
8.1.	Overview.....	48
8.1.1.	Terminal .....	49
8.1.2.	User Administration .....	49
8.1.3.	Access Control .....	49
8.1.4.	Terminal Settings .....	49
8.1.5.	Terminal .....	50
8.2.	User Administration.....	51

8.2.1.	Attendance Report .....	51
	Daily report.....	52
8.2.2.	View Event Log .....	53
8.2.2.1.	Deleting Event Logs .....	53
8.2.3.	Add Event Log.....	54
8.2.4.	View User List .....	55
8.2.4.1.	To sort:.....	56
8.2.4.2.	To Deactivate/Activate/Enable /Disable Automatch/ Users .....	56
8.2.5.	To Add New Users .....	57
8.2.5.1.	To Add A New User:.....	57
8.2.6.	Departments.....	59
8.2.6.1.	To Add a New Department: .....	59
8.2.6.2.	To Modify Existing Departments:.....	59
8.2.6.3.	To Delete Existing Departments:.....	60
8.2.7.	User Messages .....	61
8.2.7.1.	To Add a New Message: .....	61
8.2.7.2.	To delete an existing User Message: .....	61
8.2.8.	Admin Setting .....	62
8.3.	Access Control.....	63
8.3.1.	Access Groups .....	63
8.3.1.1.	To View/Delete Existing Access Groups:.....	63
8.3.1.2.	To Add a New Access Group .....	64
8.3.1.3.	To Modify an Access Group .....	64
8.3.1.4.	To Add a New Access Right.....	65
8.3.1.5.	To Delete/ Modify Access Right.....	66
8.3.2.	Triggers.....	67
8.3.2.1.	To View or Modify Existing Trigger List.....	67
8.3.3.	Holidays Settings.....	69
8.4.	Terminal Settings .....	70
8.4.1.	Terminal Setup .....	70
8.4.2.	Authentication/Log Setup .....	72
8.4.3.	Terminal List.....	74
8.4.4.	Door Open Schedule .....	75
8.4.5.	Bell Schedule .....	76
8.4.6.	Connection Profile .....	77
8.4.7.	Terminal Clock .....	77
8.4.8.	External Devices.....	78
8.4.9.	Cloud Storage Service.....	78
8.4.10.	Short Message Service(SMS) .....	78
8.4.11.	Alert Log Settings .....	79
8.4.12.	Alert Log.....	79
8.4.13.	Backup System Data .....	80
8.4.14.	Restore System Data .....	81
8.4.15.	Firmware Upgrade.....	82
8.4.16.	Download Report.....	83
8.4.17.	Capture Fingerprint .....	84
8.4.18.	Capture Picture .....	85
8.4.19.	Remote Door Open .....	86
8.4.20.	Reboot.....	87
8.4.21.	Register.....	87

Appendix A. Job code feature

Appendix B. Emergency Mode

Appendix C. SMTP server setup

Appendix D. Additional Security Options

Appendix E. Cloud Storage Service

Appendix F. Short Message Service (SMS)

Appendix G. FingerPrint enrollment notes

## Chapter 1. Introduction

This section explains the purpose and software references of the ACTAtek3.

### 1.1. Purpose

ACTAtek3 devices are the basic hardware platform of a cloud- and web-based ID management solution for security and Human Resource Management. The ACTAtek3 device allows users to access its record from any where, at any time and on any ICT platform using any web-browsers such as IE, Firefox, Chrome, Safari etc.

The primary objective of this document is to provide guidance on how to use the basic and advance features of ACTAtek3.

The secondary objective of this document is to assist the user to troubleshoot the ACTAtek3 within the shortest time if any issues incurred during installation and usage. So, after read through this training manual, user will become more familiar with the functions and features of ACTAtek3.

Some of the features and functions will require working with the ACTAtek Access Manager Suite (AMS) of Software. The Emergency Exit function is intended to be used with a traditional control panel from other third parties.

### 1.2. Document Conventions

Input typed in a bold Arial font, and output using Arial. Comments are added in *italics*.

Command prompt and Source code looks like

```
main()
{
    printf("Hello World\n");
}
```

### 1.3. Intended Audience and Reading Suggestion

This document is self-contained but assumes a basic knowledge of ACTAtek3. Advanced customers can use this document to enhance their usage in ACTAtek3, and resellers can use this document to enhance their customers' needs.

### 1.4. Software References for this document

**ACTAtek3 firmware: 3\_06.1305**

## Chapter 2. Product Overview

### 2.1. ACTAtek3 Model number

Model Number	Description
ACTA3-[Model]-[Option]-[Others]	Embedded SSL-Web Server with PIN / Camera / Smart card / Fingerprint / Sample unit starting from 1,000 users

Table 1. ACTAtek3 Model Number

#### 2.1.1. Legend

Model	Meaning
10k (smartcard, camera, fingerprint)	Embedded SSL-Web Server up to 10,000 users
15k	Embedded SSL-Web Server up to 15,000 users
20k	Embedded SSL-Web Server up to 20,000 users
30k	Embedded SSL-Web Server up to 30,000 users
Option	Meaning
P	Pin Model
C	Camera Model
S (M / L / Hp / EXBC)	Smart Card Model (Mifare/ Legic / HID prox. / Barcode)
FAM / FLI	Fingerprint Model
FAM-S / FLI-S	Fingerprint + Smartcard Model
<p>Note: ACTA3 FAM model is compatible with previous ACTA2 FAM ver.6.053. Downward compatibility between ACTA3 FAM and ACTA3 models is achieved by using the AMS of software to manage both types of devices.</p> <p>Whereas ACTA3 FLI model is NOT compatible with the ACTA2 as it uses latest fingerprint recognition and other technologies.</p>	
Others	Meaning
SAM	Sample Unit

Table 2. Legend

#### 2.1.2. EXAMPLE

Model Number	Description
ACTA3-1k-PC	Pin + Camera Model (up to 1,000 users)
ACTA3-3k-SM	Smartcard Model (Mifare) (up to 3,000 users)
ACTA3-5k-FAM-C	Fingerprint Model (FAM) + Camera (up to 5,000 users)
ACTA3-1k-FLI-SM-C	Fingerprint Model (FLI)+ Smartcard Model (Mifare) + Camera (up to 1,000 users)

ACTA3-1k-FAM-SM-C	Fingerprint Model (FAM)+ Smartcard Model (Mifare) + Camera (up to 1,000 users)
-------------------	---

Table 3.Example

## 2.2. Comparison between Fingerprint and Smart Card Models:

Features	Fingerprint ONLY	Smartcard ONLY	Fingerprint + Smart Card
Seven-Finger Enrollment	√	-	√
Built-in Smart Card Reader	-	√	√
Built-in Web and Database Server	√	√	√
Built-in CMOS/Video Camera	Optional	Optional	Optional
Static IP Address Assignment	√	√	√
Support existing DHCP server	√	√	√
Operating Temperature	-5C-65C	-5C-65C	-5C-65C
Nand Flash Memory	256 MB	256 MB	256 MB
Maximum Users	25,000 Users	30,000 Users	25,000 Users
Maximum Auto-Match Users (1:N)	Up to 10,000 users	-	Up to 10,000 users
Maximum event logs stored	- 75K for 1K / 3K / 5K model - 10K for 10k model - 10K for 15k model - 10K for 20k model - 10K for 25k model	- 75K for 1K / 3K / 5K model - 10K for 10k model - 10K for 15k model - 10K for 20k model - 10K for 30k model	- 75K for 1K / 3K / 5K model - 10K for 10k model - 10K for 15k model - 10K for 20k model - 10K for 25k model
Maximum Photos stored	500	500	500
Computers Supported	Apple Macintosh / Win 95/98/NT/XP Unix Machines / Linux Machines / PDA / Smart Phone	Apple Macintosh / Win 95/98/NT/XP Unix Machines / Linux Machines / PDA / Smart Phone	Apple Macintosh / Win 95/98/NT/XP Unix Machines / Linux Machines / PDA / Smart Phone
Database Interface Support	ODBC / JDBC	ODBC / JDBC	ODBC / JDBC
Encryption	SSL	SSL	SSL
Multilingual Support	√	√	√
Programming API	SOAP	SOAP	SOAP
Reporting	√	√	√
SNMP	√	√	√
Product Weight / Gross Weight with power supply & packaging	650g/1.5kg	650g/1.5kg	650g/1.5kg
Replaceable Modules	CPU / Fingerprint / Contact & Contactless Smartcard / Keypad	CPU / Fingerprint / Contact & Contactless Smartcard / Keypad	CPU / Fingerprint / Contact & Contactless Smartcard / Keypad
External I/O board support	√	√	√

LCD Module	Color screen	Color screen	Color screen
Product Dimension	175 x 81 x 41 (mm)	175 x 81 x 41 (mm)	175 x 81 x 41 (mm)
Weatherproof Casing	√	√	√
Expansion	Serial / RS-232 / RS-485(built-in)	Serial / RS-232 / RS-485(built-in)	Serial / RS-232 / RS-485(built-in)
Wiegand Output (*shared RS-485)	√	√	√
Network Interface	100 BaseT Ethernet (Built-in) / Optional Wi-Fi	100 BaseT Ethernet (Built-in) / Optional Wi-Fi	100 BaseT Ethernet (Built-in) / Optional Wi-Fi
Safety Standard	CE, FCC, IP65,SASO	CE, FCC, IP65,SASO	CE, FCC, IP65,SASO
Case	IP65fluid-ingress, dust, salt, fog, protection	IP65fluid-ingress, dust, salt, fog, protection	IP65fluid-ingress, dust, salt, fog, protection

**Table 4.Comparison between Fingerprint and Smartcard Models**

## 2.3. Warranty:

Please fill in the Warranty Card once you received the units. For the warranty to be valid, Warranty Card MUST be mailed or e-mailed or registered at our support website after you received your ACTAtek3. You can also join our extended warranty program after the initial 12 months manufacturer warranty expired. Please consult your sales agent for details on ongoing maintenance and warranty for your units.

Please keep the left portion of the card for your reference, and mail the right portion to the office you purchased the unit from.

### Checklist

Please check that your ACTAtek3™ comes with the following, if anything is missing, please contact your dealer or us at [support@actatek.com](mailto:support@actatek.com).

- ACTAtek3 Unit
- Instructions CD
- Quick Installation Guide
- Straight Network Cable [for connection to network (hub/switch)]
- A 12V DC Switching Power Supply (Input: 100 - 240 VAC 50/60) Hz)
- 1 Power Cord [according to Country Specification]



## **2.4. Setup Requirements**

You can use any web-browser on any PC or Smart Phones. The ACTAtek devices are platform independent.

### **2.4.1. Operating System (For access via Corporate Network)**

- Windows 95/98/2000/NT/XP/Vista/Win 7
- Linux Machines
- Unix Machine
- Apple Macintosh
- PDA
- Smart Phone

### **2.4.2. Network Interface**

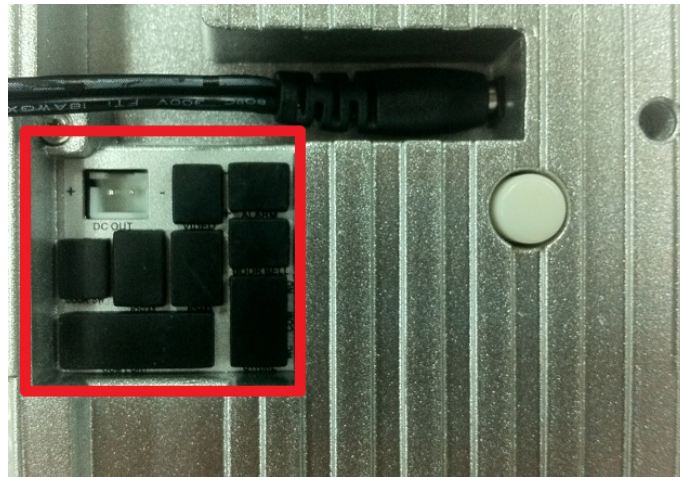
- 100 BaseT Ethernet (built-in)
- RJ45 Cabling for Network Connectivity.
- Straight Network Cable (White/Blue cable, to connect to your corporate network via Hub/Switch)
- Crossover Network Cable (Black cable, to connect directly to your Computer)

### **2.4.3. Power Requirements**

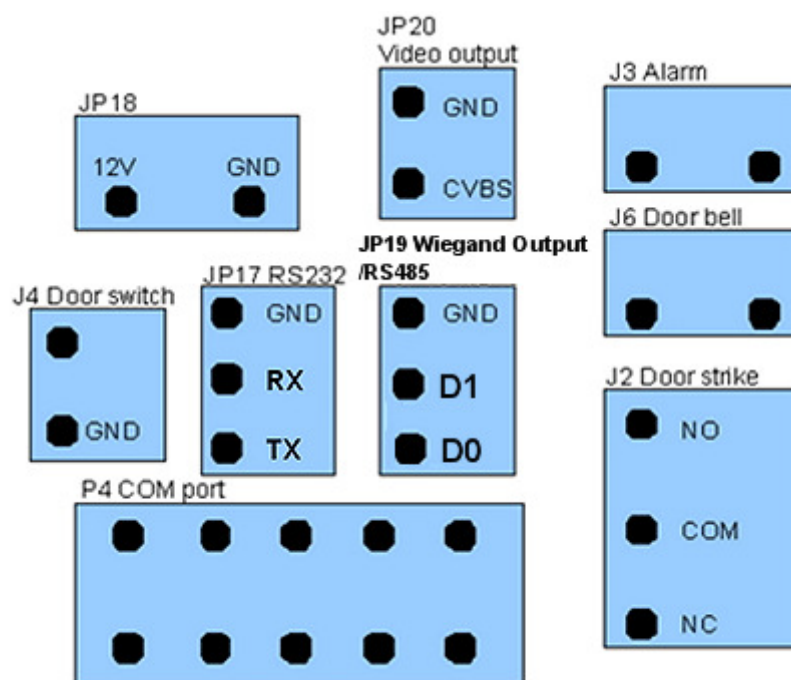
- A 12V DC switching power supply (provided), please do not substitute our power supply from another one
- Each 12V power supply can only support ONE ACTAtek3, failing to do so will void the warranty.

## Chapter 3. ACTA3 Structure and Connections

### 3.1. ACTAtek3™ Internal Structure and Connections



ACTAtek3 back panel



ACTAtek3 back panel ports

## **3.2. Connection Details:**

### **3.2.1. JP18**

- Reserved for 12V 1A power output

### **3.2.2. JP20**

- Used for video output. The video output cable can be connected to any DVR /or monitors with input via BNC connector.



### **3.2.3. J3**

- Used for alarm purpose, when the case of the unit is open, the alarm will be triggered. When it is triggered, the two pins will be short circuit.

### **3.2.4. J4**

- Used as door switch1.

### **3.2.5. JP17**

- Used for debug or connecting external IO board.

### **3.2.6. JP19**

- Support Wiegand output (\*\*on demand basis\*\*) / RS485

### **3.2.7. J6**

- Working as a doorbell. If doorbell key on the front panel is pressed, the two pins will be short circuit.

### **3.2.8. P4**

- Reserved to connect to the external barcode or magnetic strip reader.

### **3.2.9. J2**

- Used for door strike. NO (normal open) is open circuit normally, and will be short circuit when door is open. NC (normal close) is short circuit normally, and will be open circuit when door is open.

## Chapter 4. FingerPrint Notes

### 4.1. Introduction

ACTAtek3™ uses latest Optical Scanning technology with its own algorithms and matching calculations, a step above other sensors in the market.

It must be emphasized that to get an accurate enrollment and quick authentication each time a fingerprint is presented, the fingerprint placement must be towards the center of the scanner. Placing your finger far from the center position of the sensor will increase the rejection rate.

Finger Rotation should be kept to a minimum during enrollment and verification.

When enrolling, place the finger on the sensor where the entire core can clearly be seen by the scanner.

A good image is critical for the overall performance of the fingerprint scanner. Any deviation from a good image, either by placing the finger far away from the scanner, or by applying too much pressure or not locating it in the CENTER of the scanner, will cause the scanner's rejection rate to rise. Read below on how to get a good image for your enrollment /authentication.

### 4.2. Technical Information

<i>Features</i>	<i>Technical Specification</i>
Image Resolution:	500DPI
False Rejection Rate (FRR):	0.01%
False Acceptance Rate (FAR):	0.0001%
Allowable Fingerprint Rotation:	+/-15degree
Operation Temperature:	-25 to +65 Degrees Celsius
Number of minutiae being taken:	30 to 60 depending on user
Matching Speed:	0.05 second
Scanning Speed:	1.50 second

**Table 5. Technical Information**

### 4.3. *Good Image vs Bad Image*

A good fingerprint image is one in which the core of the fingerprint is well-defined and easily recognizable. The core of a finger is defined as the “point located within the inner most recurring ridge”, it is normally located in the MIDDLE of the fingerprint. It is therefore critical when enrolling that you place the finger on the scanner where the entire core can clearly be seen.

An example of a good & bad image is displayed as follows:



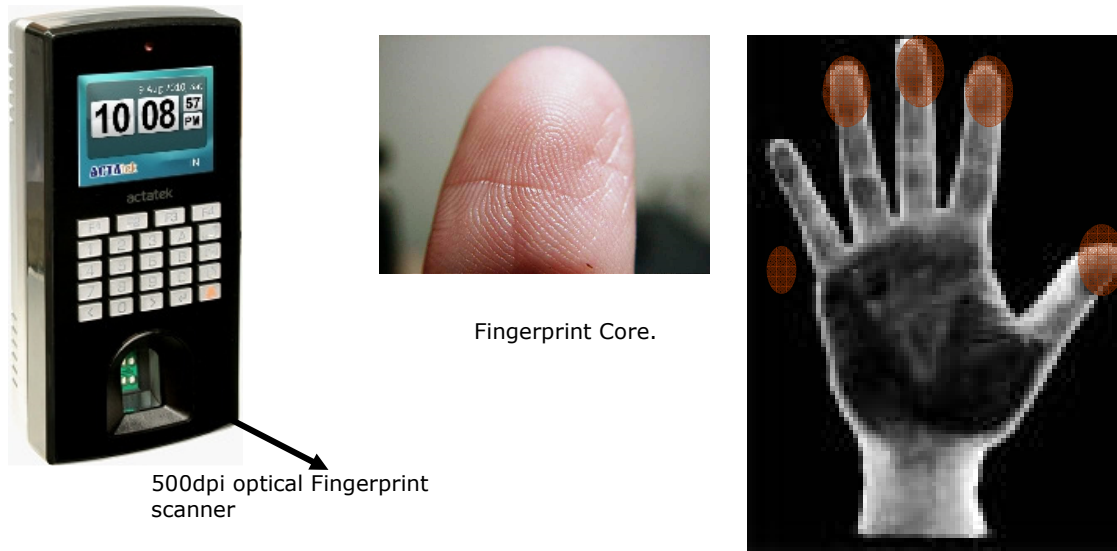
Good Image: The whole fingerprint core can be seen clearly.



Bad Image: An image where the crackles & displacement of the fingerprint core makes it unrecognizable.

#### 4.4. *Fingerprint Enrollment & Authentication*

In order to receive a successful enrollment and authentication, it is critical that the following should be noted carefully. Each successful enrollment will result in a successful authentication and save a lot of time in troubleshooting and erroneous readings.



It is highly recommended for the fingerprint core to be big and clear for a successful enrollment of a clear and good image.

Make sure the fingerprint image captured is of the core of the finger presented. A fingerprint core is a point located within the innermost recurring ridge of any given finger.

Also, to obtain a higher success rate, it was recommended to enroll the same finger 3 times in a slightly adjusted angle, one to the center, one inclined slightly to the left and the third inclined slightly to the right.

If you follow the following enrollment procedure, the success rate will increase dramatically.

#### **4.5. Fingerprint Enrollment:**

Step 1: Place the center of any one finger directly above the sensor right in the center, as shown below:



Step 2: Place the center of the same finger (enrolled in Step 1), slightly aligned to the left.

Step 3: Place the center of the same finger, slightly aligned to the right.

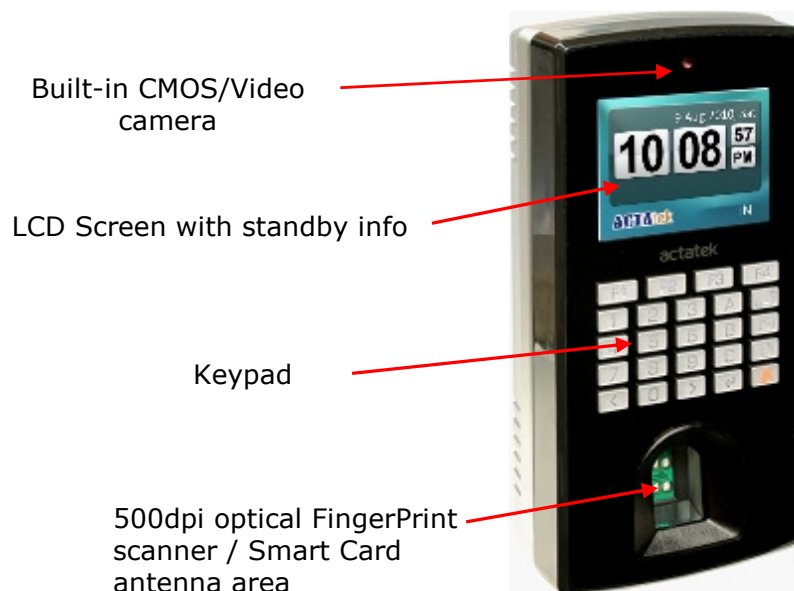
After each placement, wait for the message “Please Remove Finger” on the LCD screen to appear, and then remove your finger and then continue to enroll the second and the third finger(s). The third time will take a little longer due to the device was converting the captured image into an encrypted data.

If you have any questions regarding the above FingerPrint enrollment procedure, you can e-mail us at [support@actatek.com](mailto:support@actatek.com) or check with the sales agent.

## Chapter 5. ACTAtek3 Introduction

### 5.1. Introduction

To begin operation of your ACTAtek3™, you must make sure it is connected to a 12V DC Power supply with the network cable securely attached to the port. Once your unit is powered up, the following screen should appear, the ACTAtek logo, the system clock, the Trigger should appear in the right corner, and the date/day of the system in the up and right corner. On the next page, the keypad will be described as to how to access the unit for all the functionalities.



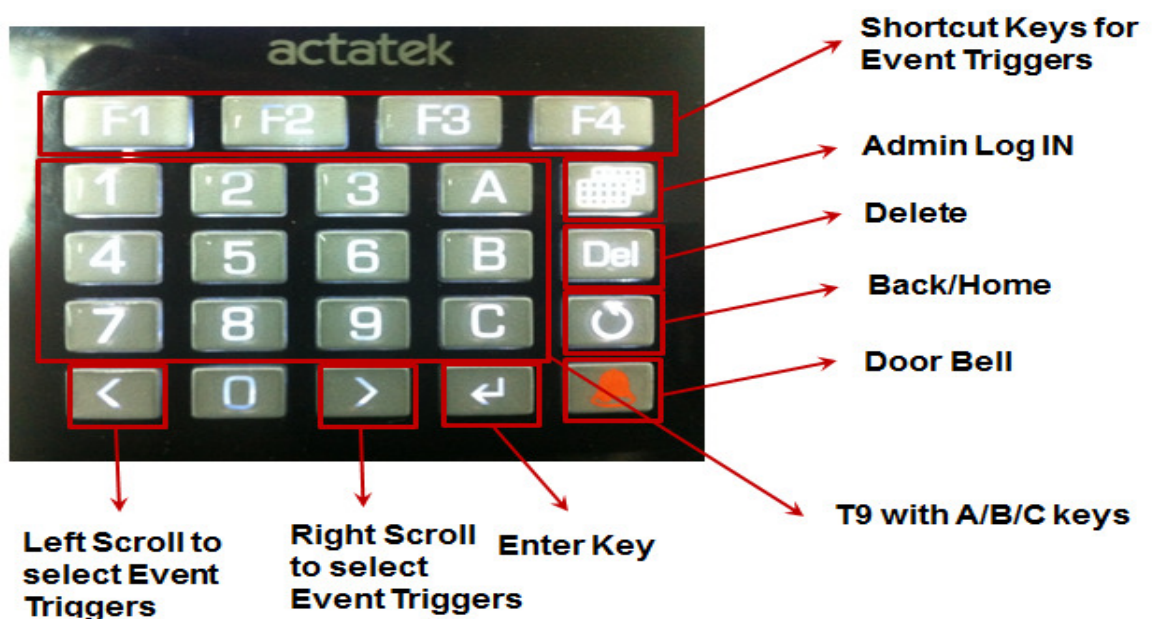
## 5.2. LCD Module

The Standby Screen displayed when the ACTAtek3™ is powered up as shown below. It has basic information such as the company logo, time, trigger type, date and day displayed when the system is idle and is not currently in use.



## 5.3. Keypad Module

The keypad module, displayed below, has various menu options and alpha-numeric keys, below is a brief description of the keypad.



## **5.4.      *Fingerprint Scanner Module***

The biometric fingerprint module uses optical scanner technology with a 500 dpi resolution and it can be accessed either with a 1:1 authentication (ID match) or 1:N authentication.(Auto-Match)

Note: The 1:N authentication(Auto-Match), although convenient, has its limitation in the maximum number of users.

With any database, the more users in the system, the slower the authentication & verification time of the unit since the system has to check its entire database for that 1 specific fingerprint for authentication. It is therefore highly recommended for users to key in their ID, and then presents their fingerprint for a much quicker & accurate verification process.

The steps for a successful enrollment have been discussed earlier in the Fingerprint Notes section, for more information on the scanner and its technology; please refer to Chapter 4 on Fingerprint Notes.

## Chapter 6. System Configuration

### 6.1. Login

#### Login to the ACTAtek3™ Admin System

There are two ways for a Super Administrator to log in to the ACTAtek3 system, one is by fingerprint, and the other is by password.

##### **Logging in via Password:**

- Press the [Admin Menu Button] on the keypad of your ACTAtek3™ unit.
- The system will prompt for the Admin ID. (Default: A999),
- Press Enter / Return
- The system will prompt for the Password. (Default: 1)
- Press Enter / Return, and you will see the Administration Menu.

##### **Logging in via Fingerprint:**

- Press the Admin Menu Button on the keypad of your ACTAtek3™ unit.
- The system will prompt for the Admin ID. (Default: A999),
- Place your enrolled finger on the scanner. (Note: Make sure you had enrolled Admin's finger before.)
- Once successfully enrolled, you will see the Administration Menu.

Login
Admin ID: .....

Login
Enter Password: .....

- Once logged into the system, a number of different actions can be performed, ranging from:
- Adding New Users via Fingerprint/Password/Smart Card.
- Managing Users by Activating/Deactivating/Deleting Users from the system.
- Configuration of Fingerprint Options, such as Auto Match and Fingerprint Capture.
- Configuration of the Date & Time of the system.
- Managing the network settings, including IP assignment, Subnet Mask, DNS, and so on.
- Resetting the system and other miscellaneous terminal settings can also be done.

Each of these steps will be discussed in detail in the following sections, starting from Adding a new user to Exiting from the system.

### Changing the Default ID & Password:

The first thing to do with the unit is to change the Administrator ID & password, to do so:

1. Log in to the web interface using a web browser. (Make sure the ACTAtek3™ is connected to the network). The device's default IP address is <http://192.168.1.100/>
2. Default ID: **A999**, Default Password: **1**, **Super Administrator**, and click OK
3. Go to "View User List", click on the ID "A999".
4. Enter the new Administrator ID, and Password, and click "Modify". (The name and other details can also be changed here either now or later)

## 6.2. Add User

### 6.2.1. Adding A New User via Fingerprint

- After successfully entering the Administrator Menu, select the first icon on the top left of the screen, which is for Adding A New User.

Add User	Add User (FP)
Fingerprint Smartcard Password Return	Enter ID: .....

- Press Enter/Return
- Press Previous/Next until "Fingerprint" is Highlighted
- Press Enter/Return
- Enter the ID for the new user, e.g. AB01 (minimum 3 characters)
- Press Enter/Return

Fingerprint	OK	Fingerprint
Finger 1/3 Wait for Finger	✓ Please Remove Finger	Finger 2/3 Wait for Finger

- 3 Fingerprint Templates (default) will be requested, 3 images of 1 finger must be enrolled.
- After each successful enrollment, the "Please Remove Finger" message will be displayed,
- Enroll the second and third fingerprints by placing the finger on the sensor, and allow it to process.

OK	Fingerprint	Complete
✓ Please Remove Finger	Finger 3/3 Wait for Finger	✓ User Automatch Added Please press ENTER

- After successful enrollment of the third fingerprint, the message "User Automatch Added" will be displayed.  
Press Enter/Return to add another user, or Press the Menu button to go back to the Administrator Menu Screen, or press Back twice to exit from the system.

*Note: Starting from Firmware 1305, the User's Auto-Match will automatically enable after FinerPrint enrollment*

### 6.2.2. Adding A New User via Smart Card

- After successfully entering the Administrator Menu, select the first icon on the top left of the screen, which is for Adding A New User.

Add User
Fingerprint
Smartcard
Pass word
Return

Smartcard
Add user
Copy to Smartcard
Move to Smartcard
Copy to Terminal
Delete Smartcard

- Press 'Enter/Return'
- Press 'Previous/Next' until "Smart Card" is Highlighted
- Press 'Enter/Return'
- Use the 'Previous/Next' buttons to highlight "New User".
- Press 'Enter/Return'
- Enter the ID for the new user, e.g. 611 (minimum 3 characters)
- Press 'Enter/Return'

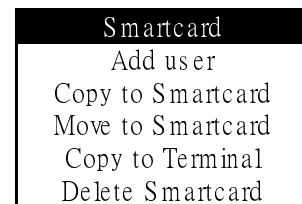
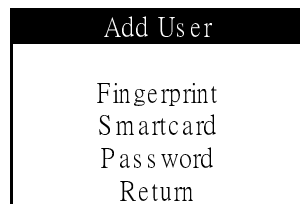
Add User (Smartcard)
Enter ID: .....

OK
✓ Success

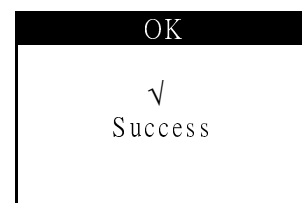
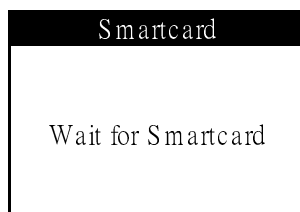
- Place the smart card over the scanner.
- If successful, the write progress will be completed and "Success" will be displayed.

### 6.2.3. *Deleting A Smart card user*

- After successfully entering the Administrator Menu, select the first icon on the top left of the screen, which is for Adding A New User.



- Press 'Enter/Return'
- Press 'Previous/Next' until "Smart Card" is Highlighted
- Press 'Enter/Return'
- Use the 'Previous/Next' buttons to highlight "Delete Smartcard".



- Place the smart card over the scanner.
- If successful, the delete progress will be completed and "Success" will be displayed. The card will then be available for use for another user.

Note:

--For FLI model, it would be required to have Mifare 4K card to be able to Copy/Remove user's FingerPrint data to the card

--For FAM model, it would be required to have MiFare 1K card to be able to Copy/Remove user's FingerPrint data to the card.

#### 6.2.4. Adding A New User via Password

- After successfully entering the Administrator Menu, select the first icon on the top left of the screen, which is for adding a New User.
- Press Enter/Return

Add User
Fingerprint
Smartcard
Pass word
Return

Add User
Enter ID: .....

- Press Previous/Next until "Password" is Highlighted
- Press Enter/Return
- Enter the ID for the new user, e.g. AB03 (minimum 3 characters)
- Press Enter/Return

Set Pass word
Enter Password: .....

OK
✓ Success

- Enter a unique password for the new user, e.g. 234
- Press Enter/Return
- Once addition is completed, the "Success!" message will be displayed.
- Press Enter/Return to add another user, or Press the Menu button to go back to the Administrator Menu Screen, or press Back twice to exit from the system.

### 6.3. Error Messages

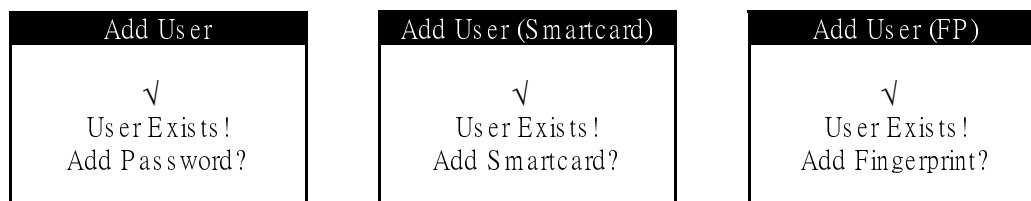
#### Beware Of..



A "Bad Quality" warning will be displayed if the fingerprint enrolled is not of acceptable quality by the system.

The reasons for the message could be manifold, either due to too little pressure on the sensor, or too much pressure on the sensor, both of which could result in an inaccurate reading of the fingerprint captured.

Another reason could be the placement of the finger is not correct, or the finger you are enrolling does not have a good fingerprint core to capture a good image. It is recommended that you do not use the pinky finger for registration and use either one of the other 4 fingers.



A "User Exist" warning will be displayed if you add the same ID that previously exists in the unit.

To avoid running into this problem, please make sure that all user ID's assigned are unique and that they are not randomly assigned.

Also, to override users, you can press Enter/Return or press Back to cease any override, and re-enter a unique user ID.

A999 cannot be used as a new ID since it is the system default's Administrator ID.

**1. Access Denied**

This message will be displayed when and if the user provides invalid login information, such as invalid ID, password, fingerprint or smart card.

**2. Unauthorized**

This message will be displayed when the user tries to login during an unauthorized time period. (For information about access groups and time settings, please refer to Access Group chapter.). In addition, if users do not have access to a particular terminal, and they try to access it, they will receive the “Unauthorized” message.

## 6.4. User Management

### 6.4.1. User Management – Activating A User

- After enrolling a few users into the system, you can manage them with the User Management option under the Administrator Menu.
- Select the second icon on the top left of the screen, which is for User Management.
- To activate a user, press the Previous or Next buttons until “Activate User” has been highlighted.
- Press Enter/Return
- Enter the User ID for activation, e.g. 123
- Press Enter/Return
- If the user exists, and is successfully activated, the above screen will be displayed.
- Press Enter/Return to activate another user, or Press the Menu button to go back to the Administrator Menu Screen, or press Back twice to exit from the system.

User Manager	Activate	OK
Activate User Delete User Deactivate User View Log Capture FP	Activate ID: .1.....	✓ Success

*Note: After enrolling new users (FingerPrint / Smart Card or Password), all new users were activated already. It will not be required to activate all new users again.*

### 6.4.2. User Management – Deactivating A User

- After enrolling a few users into the system, you can manage them with the User Management option under the Administrator Menu.
- Select the second icon on the top left of the screen, which is for User Management.
- To deactivate a user, Press the Previous or Next buttons until “Deactivate User” has been highlighted.
- Press Enter/Return
- Enter the User ID for deactivation, e.g. 123
- Press Enter/Return

User Manager	Deactivate	OK
Activate User Delete User Deactivate User View Log Capture FP	Deactivate ID: .1.....	✓ Success

- If the user exists, and is successfully deactivated, the above screen will be displayed.
- Press Enter/Return to deactivate another user, or Press the Menu button to go back to the Administrator Menu Screen, or press Back twice to exit from the system.

### 6.4.3. User Management – Deleting A User

- After enrolling users into the system, you can manage them with the User Management option under the Administrator Menu.
- Select the second icon on the top left of the screen, which is for User Management.
- To Delete a user, press the Previous or Next button until “Delete User” has been highlighted.
- Press Enter/Return
- Enter the User ID for deleting
- Press Enter/Return

User Manager
Activate User
Delete User
Deactivate User
View Log
Capture FP

Delete
Delete ID: .....

OK
√ Success

- If the user exists, and is successfully deleted, the above screen will be displayed .Press Enter/Return to delete another user, or Press the Menu button to go back to the Administrator Menu Screen, or press Back twice to exit from the system.\*

*\*WARNING: Deleting a user will remove ALL of his/her information from the system, including access logs, and personal details. Please make sure that you have backed up the information before making any changes to the user list, just so you have something to roll back to.*

## 6.5. Auto Match

### Auto Match – Enable/Disable

After enrolling users into the system via fingerprint, Auto Match may be enabled for individual users. The primary function of Auto Match is to allow users to access the system without inputting their ID first. All they need to do to gain access is to place their fingers on the scanner and let the ACTAtek3™ do the rest. Verification is quicker if few people are enrolled into the system, and if few people are allowed to use the Auto Match feature. It is highly recommended that Auto match be limited in use and if used for all users, it should be understood that the verification time will be longer than if you input your ID and then fingerprint. Authentication methods are discussed in earlier sections.

### 6.5.1. To Enable Auto Match

- Select the third icon on the top left of the screen, which is for Auto Match
- Press 'Enter/Return' once "Auto Match" is highlighted.

Automatch	Automatch	OK
Automatch Group Automatch Return	Enter ID: .....	√ Automatch Enabled

- Enter the ID of the user for whom Auto Match is being enabled, e.g. 123.
- Press 'Enter/Return'.
- If the user exists in the system, and their Auto Match function was not previously enabled, the message "Automatch Enabled!" will be displayed.
- Press 'Enter/Return' to enable Auto Match for another user, or Press the 'Menu' button to go back to the Administrator Menu Screen, or press 'Back' twice to exit from the system.

### 6.5.2. To Disable Auto Match

- Select the third icon on the top left of the screen, which is for Auto Match
- Press 'Enter/Return' once "Auto Match" is highlighted.

Automatch	Automatch	OK
Automatch Group Automatch Return	Enter ID: .....	√ Automatch Disabled

- Enter the ID of the user for whom Auto Match is being disabled, e.g. 123.
- Press 'Enter/Return'.
- If the user exists in the system, and has previously enabled their Auto Match function, the message "Automatch Disabled!" will be displayed.
- Press 'Enter/Return' to disable Auto Match for another user, or Press the 'Menu' button to go back to the Administrator Menu Screen, or press 'Back' twice to exit from the system.

## 6.6. *Date & Time*

### Date & Time Function

ACTAtek3™ can be used as both an Access Control system, as well as a Time Attendance System. For this reason, it is critical to set the correct date & time function, so that the unit works and records the correct time of the attendance data for payroll or other HR purposes. This part shows how to make changes to the Date & Time function directly at the unit.

### 6.6.1. *To Modify the Date Settings*

- Select the icon on the top right of the screen, which is for Date & Time Settings.
- Press 'Enter/Return' once "Date & Time" is highlighted.
- Press the 'Previous and Next Button'(s) until the "Adjust Date" option is highlighted.
- Press 'Enter/Return'
- This shows the Current Date of the System, and you can enter the New Date to modify it in YYYY/MM/DD format.
- Press 'Enter/Return' to Save, if successful, the below screen with the message "Date Adjusted" will appear.

Date & Time	Adjust Date	Adjust Date
Adjust Date Adjust Time Return	Current: 2010/05/19 New: 2010/05/19 (YYYY/MM/DD)	√ Date Adjusted

- Press 'Enter/Return' to modify the Time or other settings, or Press the 'Menu' button to go back to the Administrator Menu Screen, or press 'Back' twice to exit from the system.

### 6.6.2. To Modify the Time Settings

- Select the icon on the top right of the screen, which is for Date & Time Settings.
- Press 'Enter/Return' once "Date & Time" is highlighted.
- Press the 'Previous and Next Button'(s) until the "Adjust Time" option is highlighted.
- Press 'Enter/Return'
- This shows the Current Time of the System, and you can enter the New Time to modify it in HH:MM:SS format.
- Press 'Enter/Return' to Save, if successful, the below screen with the message "Time Adjusted" will appear.

Date & Time	Adjust Time	Adjust Time
Adjust Date Adjust Time Return	Current: 15:46:50 New: 16:00:00 (HH:MM:SS)	√ Time Adjusted

- Press 'Enter/Return' to modify other settings in the Date & Time Menu option, or Press the 'Menu' button to go back to the Administrator Menu Screen, or press 'Back' twice to exit from the system.

## 6.7. IP Settings

### IP Settings Function

ACTAtek3™ is a web-based system, and works similarly as a network appliance. Having say that, it has its own IP Address assignment, either by using Dynamic or Static Assignment. This will allow the administrator to access the device Web UI via any browsers such as Internet Explorer, Firefox, or Chrome etc. without much hassle, as long as it is in the same network as the corporate LAN (Local Area Network) or set the device's IP address to access from Internet. Below are the basic steps on how the IP Address for the ACTAtek3™ unit can be modified, so as to enable communication from the browsers.

### 6.7.1. IP Address Configuration

- Select the icon on the bottom left of the screen, which is for IP Settings.
- Press 'Enter/Return' once IP Settings is highlighted.
- Press the 'Previous/Next' buttons to highlight "IP Address", press 'Enter/Return'.
- Once selected, the Current IP Address will be displayed, and the new modification can take place.
- Enter the New IP Address and Press 'Enter/Return'.
- If successful, a "Success" message will be displayed.

IP Setting	IP Address	OK
DHCP (OFF)		
Subnet Mask	Current: 192.168.1.100	√
IP Address	New: 192.168.1.200	Success
Gateway		
DNS IP		

- Press 'Enter/Return' to modify other settings in the IP Settings option, or Press the 'Menu' button to go back to the Administrator Menu Screen, or press 'Back' twice to exit from the system.

### 6.7.2. Default Gateway Configuration

- Select the icon on the bottom left of the screen, which is for IP Settings.
- Use the 'Previous / Next' button until the "Gateway" option is highlighted
- Press 'Enter/Return'
- The Current Default Gateway address will be displayed
- The New Default Gateway Address can be entered here.
- Once entered, press 'Enter/Return'.
- If successful, a "Success" message will be displayed.

IP Setting	Gateway Address	OK
DHCP (OFF)		
Subnet Mask	Current: 192.168.1.1	√
IP Address	New: 192.168.1.1	Success
Gateway		
DNS IP		

- Press 'Enter/Return' to modify other settings in the IP Settings option, or Press the 'Menu' button to go back to the Administrator Menu Screen, or press 'Back' twice to exit from the system.

### 6.7.3. DNS IP Configuration

- Select the icon on the bottom left of the screen, which is for IP Settings.
- Use the Previous / Next button until the DNS IP\* option is highlighted.
- Press Enter/Return
- The Current “DNS IP” address will be displayed
- The New DNS IP Address can be entered here.
- Once entered, press ‘Enter/Return’.
- If successful, a “Success” message will be displayed.

IP Setting	DNS Address	OK
DHCP (OFF)		
Subnet Mask		
IP Address	Current: 192.168.1.1	√
Gateway	New: 192.168.1.1	Success
DNS IP		

- Press ‘Enter/Return’ to modify other settings in the IP Settings option, or Press the ‘Menu’ button to go back to the Administrator Menu Screen, or press ‘Back’ twice to exit from the system.

\*Note: DNS IP is used to resolve Domain Names to IP Address and vice versa.

### 6.7.4. Subnet Mask Configuration

- Select the icon on the bottom left of the screen, which is for IP Settings.
- Use the Previous / Next button until the Subnet Mask option is highlighted.
- Press Enter/Return
- The Current “Subnet Mask” address will be displayed
- The New Subnet Mask Address can be entered here.
- Once entered, press ‘Enter/Return’.
- If successful, a “Success” message will be displayed .

IP Setting	Subnet Mask	OK
DHCP (OFF)		
Subnet Mask	Current: 255.255.255.0	√
IP Address	New: 255.255.255.0	Success
Gateway		
DNS IP		

- Press ‘Enter/Return’ to modify other settings in the IP Settings option, or Press the ‘Menu’ button to go back to the Administrator Menu Screen, or press ‘Back’ twice to exit from the system.

### 6.7.5. DHCP IP Configuration

DHCP Configuration allows for IP Addresses to be dynamically assigned, and match with that of the corporate LAN settings. With this option, the IP Settings do not have to be statically assigned and the process can be simplified. Below are the steps for enabling or disabling the settings.

#### 6.7.5.1. To Enable DHCP:

- Select the icon on the bottom left of the screen, which is for IP Settings.
- Use the 'Previous / Next' button until the "DHCP" option is highlighted.

<div>IP Setting</div> <div>DHCP (OFF)</div> <div>Subnet Mask</div> <div>IP Address</div> <div>Gateway</div> <div>DNS IP</div>	<div>OK</div> <div>√</div> <div>DHCP Enabled</div>	<div>IP Setting</div> <div>DHCP (ON)</div> <div>Subnet Mask</div> <div>IP Address</div> <div>Gateway</div> <div>DNS IP</div>
---	--	--

- Press 'Enter/Return'.
- The Current status of the DHCP will be displayed, if it is "DHCP (OFF)", it will be enabled. If successful, a "DHCP Enabled" message will be displayed.
- Press 'Enter/Return' to modify other settings in the IP Settings option, or Press the 'Menu' button to go back to the Administrator Menu Screen, or press 'Back' twice to exit from the system.

#### 6.7.5.2. To Disable DHCP:

- Select the icon on the bottom left of the screen, which is for IP Settings.
- Use the 'Previous / Next' button until the "DHCP" option is highlighted.
- Press 'Enter/Return'.

<div>IP Setting</div> <div>DHCP (ON)</div> <div>Subnet Mask</div> <div>IP Address</div> <div>Gateway</div> <div>DNS IP</div>	<div>OK</div> <div>√</div> <div>DHCP Disabled</div>	<div>IP Setting</div> <div>DHCP (OFF)</div> <div>Subnet Mask</div> <div>IP Address</div> <div>Gateway</div> <div>DNS IP</div>
--	---	---

- The Current status of the DHCP will be displayed, if it is "DHCP (ON)", it will be disabled. If successful, a "DHCP Disabled" message will be displayed.
- Press 'Enter/Return' to modify other settings in the IP Settings option, or Press the 'Menu' button to go back to the Administrator Menu Screen, or press 'Back' twice to exit from the system.

## 6.8. Terminal Settings

### 6.8.1. Terminal Settings Function

The terminal settings feature allows users to set the ACTAtek3™ in a multi-user environment. Moreover, the Terminal Settings option can allow users to set the Security Level from High to Low, with High Fingerprint Security allowing for maximum minutiae to be accounted for during authentication. The Low settings take the minimum number of minutiae into accounting for the lowest security level. The settings can be modified for companies who are using the system primarily for Time Attendance purposes or even for those users whose fingerprint are difficult to read.

#### 6.8.1.1. Fingerprint Security Level Settings

- Select the second icon on the bottom left of the screen, which is for Terminal Settings.
- Use the Previous / Next button until "FP Quality" is highlighted.
- Press Enter/Return

Terminal Setting
FP Quality
No. of FP Sample
Restrict IP (OFF)
Unlock Door
Reboot

FP Quality
HIGH (ON)
NORMAL
LOW
Return

- The three options to select from include: High, Normal or Low. Each of which will give you the following display messages:

OK
✓
Quality High

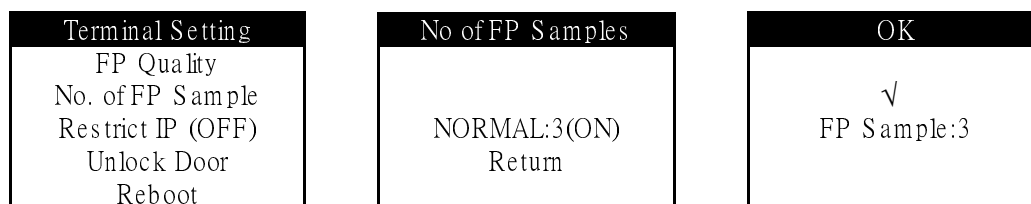
OK
✓
Quality Normal

OK
✓
Quality Low

- Press Enter/Return to modify other settings in the Terminal Settings option, or Press the Menu button to go back to the Administrator Menu Screen, or press Back twice to exit from the system.

### 6.8.2. No. of FP Sample

- Select the second icon on the bottom left of the screen, which is for Terminal Settings.
- Use the Previous / Next button until “No. of FP Sample” is highlighted.
- Press Enter/Return



- The three options to select from include: Normal:3 (default). Once selected, the system will take that number of FP templates during enrollment of new users.
- Select one and press 'Enter/Return' to save settings.
- Press Enter/Return to modify other settings in the Terminal Settings option, or Press the Menu button to go back to the Administrator Menu Screen, or press Back twice to exit from the system.

### 6.8.3. Unlock Door

- Select the second icon on the bottom left of the screen, which is for Terminal Settings.
- Use the Previous / Next button until “Unlock Door” is highlighted.
- Press Enter/Return to unlock the door.



- Press Enter/Return to modify other settings in the Terminal Settings option, or Press the Menu button to go back to the Administrator Menu Screen, or press Back twice to exit from the system.

#### 6.8.4. *System Reboot*

- Select the second icon on the bottom left of the screen, which is for Terminal Settings.
- Use the Previous / Next button until "Reboot" is highlighted.
- Press Enter/Return to reboot the unit.

Terminal Setting
FP Quality
No. of FP Sample
Restrict IP (OFF)
Unlock Door
Reboot

#### 6.9. *Reset*

##### Reset Setting Function

Resetting the User Database and Event Log can be done from the unit directly. This is essential if for some reason the company would like to remove all data from the system completely. However, it is highly recommended to make a backup of the entire database before the system has been reset.

### 6.9.1. *Resetting the Event Log*

- Select the third icon on the bottom left of the screen, which is for Reset Setting.
- Use the Previous or Next button until “Event Logs” is selected
- Press Enter/Return

Reset	Reset	OK?
Reset Event Log Reset Database Factory Deafult Reset Web Port Return	√ Reset Event Log! OK?	√ Event Log Reset!

- If successful, a “Event Log Reset!” message will be displayed.
- Press Enter/Return to modify other settings in the Reset Setting option, or Press the Menu button to go back to the Administrator Menu Screen, or press Back twice to exit from the system.

### 6.9.2. *Resetting the User Database*

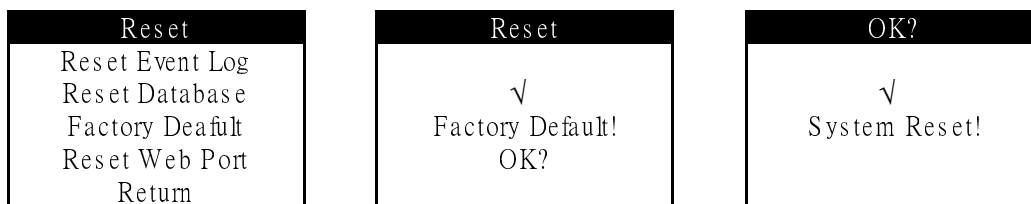
- Select the third icon on the bottom left of the screen, which is for Reset System.
- Use the Previous or Next button until “Reset Database” is selected
- Press Enter/Return

Reset	Reset	OK?
Reset Event Log Reset Database Factory Deafult Reset Web Port Return	√ Reset Database! OK?	√ Database Reset!

- If successful, a “Database Reset!” message will be displayed.
- Press Enter/Return to modify other settings in the Reset Setting option, or Press the Menu button to go back to the Administrator Menu Screen, or press Back twice to exit from the system.

### 6.9.3. *Factory Default*

- Select the third icon on the bottom left of the screen, which is for Reset System.
- Use the Previous or Next button until “Factory Default” is selected.
- Press Enter/Return
- A message “System Reset!” will be displayed once the system has been successfully reset and rebooting.



### 6.9.4. *Web Port*

- Select the third icon on the bottom left of the screen, which is for Reset System.
- Use the Previous or Next button until “Reset Web Port” is selected.
- Press Enter/Return
- A message “Web Port Reset!” will be displayed once the system has been successfully reset.



## 6.10. *Exit*

### Exit Function

Once all your settings have been completed, you can either exit the system using the Back button on the keypad or by using the Exit option in the Administration Menu.

- Select the icon on the bottom right of the screen, which is to Exit from the Admin Menu.
- Press Enter/Return, and the Standby Mode will be displayed.

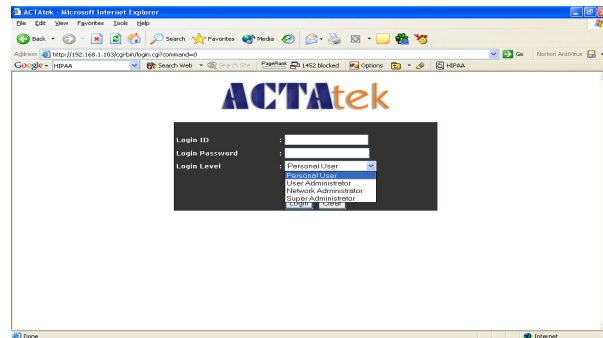
## Chapter 7. Web Administration

### Introduction

ACTAtek3™ is using TCP/IP network protocol with its embedded web server technology, which allows the administrator to have remote access via any standard web browser, e.g. Internet Explorer or Firefox. We will use Internet Explorer as our demonstrative guide; it works the same way for Firefox or any other standard web browser e.g. Chrome/Safari.

ACTAtek3™ permits for 4 access levels:

- Personal User
- User Administrator
- Network Administrator
- Super Administrator



### Personal User

The personal user login only allows for users to check their attendance records, and view their reports. No changes or modification is admissible through this configuration option. This is for employees who wish to check their attendance records or other reports generated by the system.

### User Administrator

The user administrator access level lists a different set of configuration changes that can be made to pertain to HR or Payroll requirements. The changes can be made to Access levels of different departments, addition and monitoring of job functions, reporting, as well as, managing the employee list. Add / Delete of employees can be done here, restricting access to doors for different employees can also be done by the user administrator.

### Network Administrator

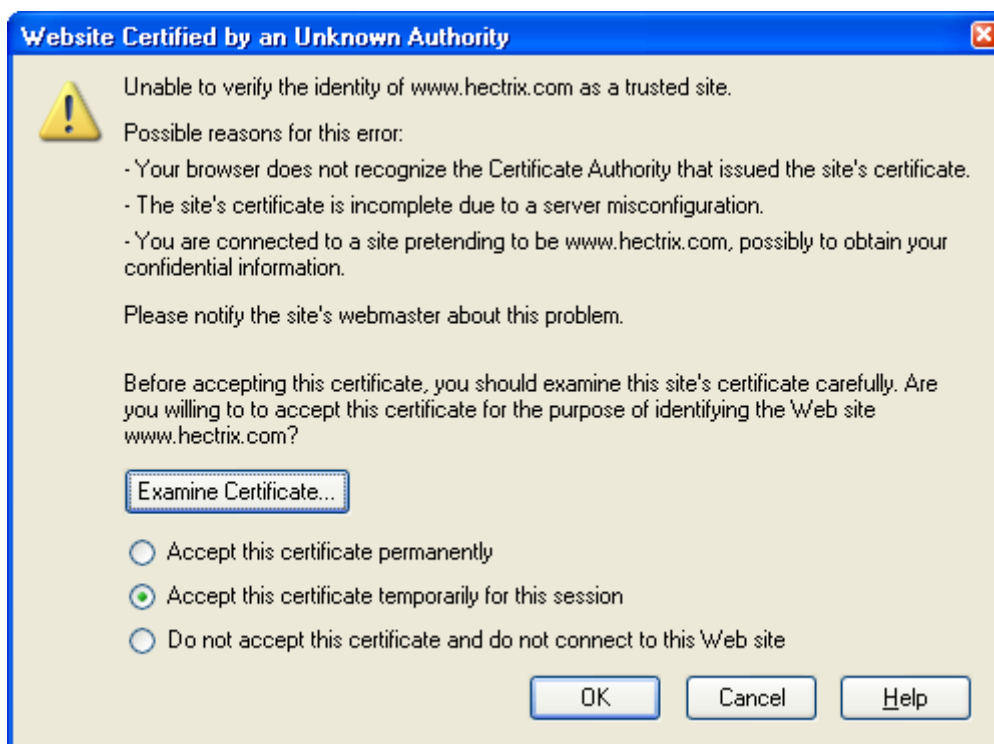
The network administrator is in charge of system configurations, such as, networking settings, terminal settings, clock setups, or password setups. Everything that involves technical knowing will be done by the network administrator. This role is usually assigned to a tech-savvy person, who is capable of making appropriate configuration changes and has basic knowledge of networking setup and IT-related issues.

### Super Administrator

The super administrator login combines the functions of 1 - 3, so the administrator is in charge of the whole system, including technical and administration functionalities. This guide is focusing on the Super Administrator usage which essentially covers all the functions.

## 7.1. SSL Certification – Data Encryption

When <http://192.168.1.100> (default IP Address of the ACTAtek3™ unit) is typed on the address bar of IE or Firefox or any other web browser, the login page will appear. Click on “Secure” to login using secure SSL data encryption, so that ALL the exchange of data is encrypted and secure.



After selecting “Secure” login, the above screen will be displayed and to go on to login to view the web interface of ACTAtek3, select either “Accept this certificate permanently” or “Accept this certificate temporarily for this session”. It is recommended to have the temporarily selected if you are not using your PC / laptop for this http session, so that others cannot use this site without the proper authentication. Make the selection and click “OK”.

If you do not wish to continue in secure mode, select “Do not accept this certificate and do not connect to this Web site”, or simply click “Cancel”.

The login page will reappear, input the login ID and password, and login level to proceed.

## 7.2. Terminal Status

**ACTAtek** The worldwide leader in Web based technologies.

<b>Terminal</b> <ul style="list-style-type: none"> <li>Log Off</li> <li><b>Terminal Status</b></li> </ul> <b>User Administration</b> <ul style="list-style-type: none"> <li>Attendance Report</li> <li>Daily Report</li> <li>View Event Log</li> <li>Add Event Log</li> <li>View User List</li> <li>Add New User</li> <li>Departments</li> <li>User Messages</li> <li>Admin Setting</li> </ul> <b>Access Control</b> <ul style="list-style-type: none"> <li>Access Groups</li> <li>Triggers</li> <li>Holidays Setting</li> </ul> <b>Terminal Settings</b> <ul style="list-style-type: none"> <li>Terminal Setup</li> </ul>	<h3>Terminal Status</h3> <table border="1"> <tr> <td>Model Number</td> <td>ACTA3- 1K-FLI-SM-C</td> </tr> <tr> <td>Serial Number</td> <td>00111DA040C3</td> </tr> <tr> <td>Firmware Version</td> <td>actatek_3_06.1305</td> </tr> <tr> <td>FLI Version</td> <td>2.050</td> </tr> <tr> <td>Terminal Description</td> <td>ACTAtek</td> </tr> <tr> <td>IP Address</td> <td>192.168.1.100</td> </tr> <tr> <td>Primary/Secondary Unit</td> <td>Primary</td> </tr> <tr> <td>System Uptime</td> <td>32 Minute(s)</td> </tr> <tr> <td>Registered/Maximum Users</td> <td>8/1000</td> </tr> <tr> <td>Automatch Users</td> <td>7/1000</td> </tr> <tr> <td>Current Status</td> <td>Online</td> </tr> <tr> <td>Last Time Server Sync Time</td> <td>Time Server Disabled</td> </tr> <tr> <td>Total Flash Memory Size</td> <td>253.38M</td> </tr> <tr> <td>Memory Free</td> <td>193.40M</td> </tr> </table>	Model Number	ACTA3- 1K-FLI-SM-C	Serial Number	00111DA040C3	Firmware Version	actatek_3_06.1305	FLI Version	2.050	Terminal Description	ACTAtek	IP Address	192.168.1.100	Primary/Secondary Unit	Primary	System Uptime	32 Minute(s)	Registered/Maximum Users	8/1000	Automatch Users	7/1000	Current Status	Online	Last Time Server Sync Time	Time Server Disabled	Total Flash Memory Size	253.38M	Memory Free	193.40M
Model Number	ACTA3- 1K-FLI-SM-C																												
Serial Number	00111DA040C3																												
Firmware Version	actatek_3_06.1305																												
FLI Version	2.050																												
Terminal Description	ACTAtek																												
IP Address	192.168.1.100																												
Primary/Secondary Unit	Primary																												
System Uptime	32 Minute(s)																												
Registered/Maximum Users	8/1000																												
Automatch Users	7/1000																												
Current Status	Online																												
Last Time Server Sync Time	Time Server Disabled																												
Total Flash Memory Size	253.38M																												
Memory Free	193.40M																												

The first page displayed, as above, will be the same no matter which login is chosen. It will show a brief status of the terminal. The information displayed includes:

Feature	Description
Model Number	The Model Number of your ACTAtek3™ unit.
Serial Number	The Serial Number of your ACTAtek3™ unit.
Firmware Version	The software version installed in the unit.e.g.3_06.1305
FAM /FLI Version	The Fingerprint Software version installed in the unit.e.g.2.050
Terminal Description	A brief description of the terminal.
IP Address	The IP address assigned to the unit, Default: 192.168.1.100
Primary / Secondary Unit	ACTAtek 3 will all behave as Primary unit.
System Uptime	This informs you how long the system has been operating without a reboot
Registered/Maximum users	This informs you how many users are Registered and the maximum no. of users supported by the unit
Automatch Users	Number of users enabled with Automatch Feature. -FAM model: up to 1,000 users (500users:default) -FLI mode: up to 10,000 users
Current Status	The current status of the unit.
Las Time Server sync time using SNTP	The last time when the device sync. its time with SNTP server if SNTP server was enable at Terminal Clock setting.
Total Flash Memory	The total memory size of the unit.
Memory Free	The memory free on the unit.

## Chapter 8. Super Administration Guide

### 8.1. Overview

After logging in under Super Administrator (Default ID: A999, password: 1), the left panel will differ from the other administrator(s), as can be seen below. All options will be available for configuration and modification of the system and user configurations.

**ACTAtek** The worldwide leader in Web based technologies.

Terminal	Terminal Status																												
<ul style="list-style-type: none"> <li>Log Off</li> <li>Terminal Status</li> </ul>																													
<b>User Administration</b> <ul style="list-style-type: none"> <li>Attendance Report</li> <li>Daily Report</li> <li>View Event Log</li> <li>Add Event Log</li> <li>View User List</li> <li>Add New User</li> <li>Departments</li> <li>User Messages</li> <li>Admin Setting</li> </ul>	<table border="1"> <tbody> <tr> <td>Model Number</td> <td>ACTA3- 1K-FLI-SM-C</td> </tr> <tr> <td>Serial Number</td> <td>00111DA040C3</td> </tr> <tr> <td>Firmware Version</td> <td>actatek_3_06.1305</td> </tr> <tr> <td>FLI Version</td> <td>2.050</td> </tr> <tr> <td>Terminal Description</td> <td>ACTAtek</td> </tr> <tr> <td>IP Address</td> <td>192.168.1.100</td> </tr> <tr> <td>Primary/Secondary Unit</td> <td>Primary</td> </tr> <tr> <td>System Uptime</td> <td>32 Minute(s)</td> </tr> <tr> <td>Registered/Maximum Users</td> <td>8/1000</td> </tr> <tr> <td>Automatch Users</td> <td>7/1000</td> </tr> <tr> <td>Current Status</td> <td>Online</td> </tr> <tr> <td>Last Time Server Sync Time</td> <td>Time Server Disabled</td> </tr> <tr> <td>Total Flash Memory Size</td> <td>253.38M</td> </tr> <tr> <td>Memory Free</td> <td>193.40M</td> </tr> </tbody> </table>	Model Number	ACTA3- 1K-FLI-SM-C	Serial Number	00111DA040C3	Firmware Version	actatek_3_06.1305	FLI Version	2.050	Terminal Description	ACTAtek	IP Address	192.168.1.100	Primary/Secondary Unit	Primary	System Uptime	32 Minute(s)	Registered/Maximum Users	8/1000	Automatch Users	7/1000	Current Status	Online	Last Time Server Sync Time	Time Server Disabled	Total Flash Memory Size	253.38M	Memory Free	193.40M
Model Number	ACTA3- 1K-FLI-SM-C																												
Serial Number	00111DA040C3																												
Firmware Version	actatek_3_06.1305																												
FLI Version	2.050																												
Terminal Description	ACTAtek																												
IP Address	192.168.1.100																												
Primary/Secondary Unit	Primary																												
System Uptime	32 Minute(s)																												
Registered/Maximum Users	8/1000																												
Automatch Users	7/1000																												
Current Status	Online																												
Last Time Server Sync Time	Time Server Disabled																												
Total Flash Memory Size	253.38M																												
Memory Free	193.40M																												
<b>Access Control</b> <ul style="list-style-type: none"> <li>Access Groups</li> <li>Triggers</li> <li>Holidays Setting</li> </ul>																													
<b>Terminal Settings</b> <ul style="list-style-type: none"> <li>Terminal Setup</li> <li>Authentication/Log Setup</li> <li>Terminal List</li> <li>Door Open Schedule</li> <li>Bell Schedule</li> <li>Connection Profile</li> <li>Terminal Clock</li> <li>External Devices</li> </ul>																													
<b>Terminal</b> <ul style="list-style-type: none"> <li>Cloud Storage Service</li> <li>SMS Service</li> <li>Alert Log</li> <li>Syslog</li> <li>Backup System Data</li> <li>Restore System Data</li> <li>Firmware Upgrade</li> <li>Download Report</li> <li>Capture Fingerprint</li> </ul>																													

The System Administrator is usually the person who is in charge of the whole system, which includes the networking and technical side of works, as well as the HR and administration side. The Super administrator option is either a top executive who has control over the company data and knows the technical aspect too. Moreover, for small companies the roles of both the User and Network administrator(s) may be combined to one, and this is main role of the Super Administrator.

From the left panel, the user administrator will be able to choose from the following:

### **8.1.1. Terminal**

- |                    |                                       |
|--------------------|---------------------------------------|
| 1. Log off         | - To log off from the system.         |
| 2. Terminal Status | - To view the overall terminal status |

### **8.1.2. User Administration**

- |                      |  |
|----------------------|--|
| 1. Attendance Report | - To view the attendance report of users in the system.  |
| 2. Daily Report      | - To view the daily report of users in the system  |
| 3. View Event Log    | - To view the event log of the users in the system   |
| 4. Add Event Log     | - To add an event log into the system  |
| 5. View User List    | - To view the list of users in the system  |
| 6. Add New User      | - To add a new user into the system  |
| 7. Departments       | - To view the list of departments or add a new department  |
| 8. User Messages     | - To send the personalized messages to individual users during clock IN/OUT.(Standalone mode)                                      |
| 9. Admin Setting     | - Super Administrator can set access rights for "Personal User" &"System Administrator" to View Event Log or View/Download Reports |

### **8.1.3. Access Control**

- |                     |  |
|---------------------|--|
| 1. Access Groups    | - To view or modify existing access groups or add a new group        |
| 2. Triggers         | - To view or modify the trigger list.                                |
| 3. Holidays Setting | - To setup the systems for recognizing holidays for unique settings. |

### **8.1.4. Terminal Settings**

- |                               |  |
|-------------------------------|--|
| 1. Terminal Setup             | - To view modify the terminal settings, e.g. IP / Gateway.                                     |
| 2. Authentication / Log Setup | - To setup the behavior of authentication log.   |
| 3. Terminal List              | - To view the list of terminals connected.   |
| 4. Access Client Setup        | - To setup the ACTAtek to register with Access Manager. ( <i>Under [Access Manager] mode</i> ) |
| 5. Door Open Schedule         | - To view or modify the door opening schedule.   |
| 6. Bell Schedule              | - To view or modify the bell schedule period.  |

- |                                  |   |
|----------------------------------|---|
| 7. Connection Profile (reserved) | - Use for manual Agent configuration.                 |
| 8. Terminal Clock                | - To view or modify the terminal clock settings.      |
| 9. External Devices              | - To connect external I/O board to the ACTAtek3 unit. |

### **8.1.5. Terminal**

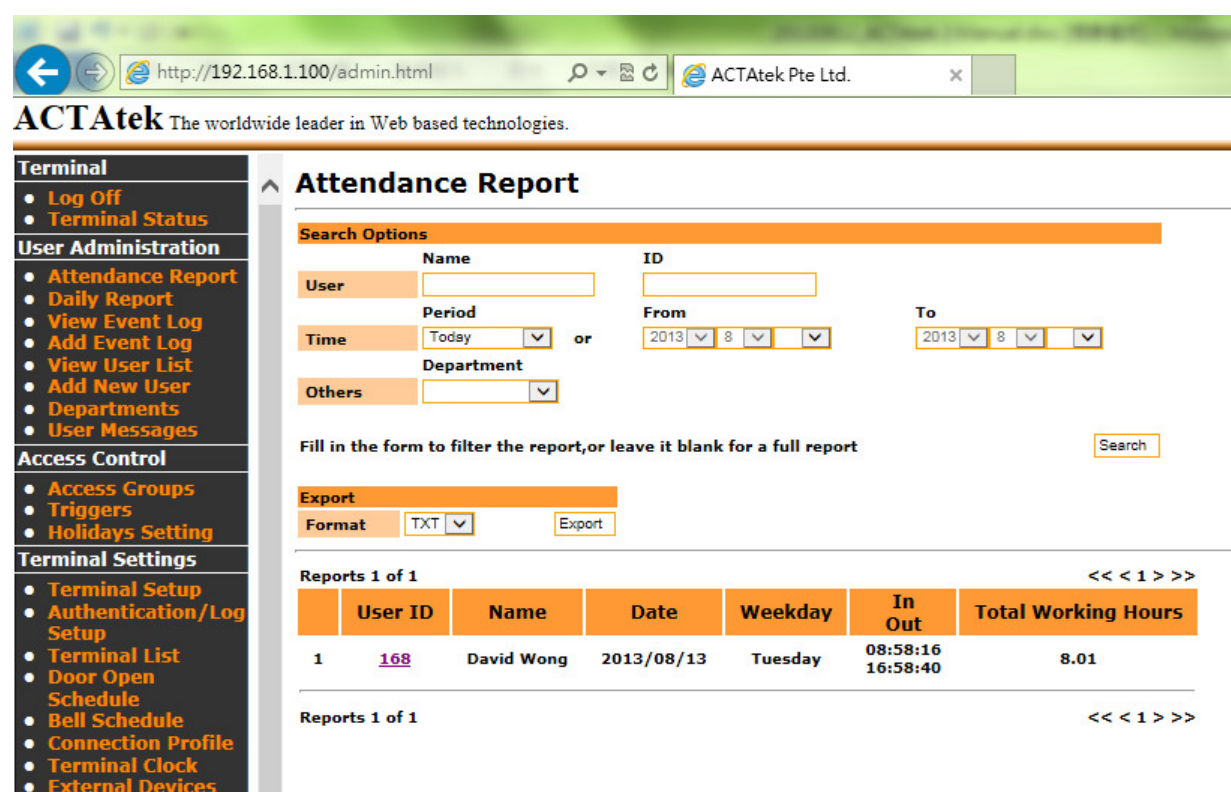
- |                          |   |
|--------------------------|---|
| 1. Cloud Storage Service | - Google Drive Spreadsheet integration                                    |
| 2. SMS Service           | -To setup the SMS service   |
| 3. Alert Log             | -To setup which action gives out alert log                                |
| 4. Syslog                | -To enable the remote system log  |
| 5. Backup System Data    | - To backup the system data.  |
| 6. Restore System Data   | -To restore the system data from a previous setting                       |
| 7. Firmware Upgrade      | - To upgrade the firmware or patch files provided by ACTAtek support team |
| 8. Download Report       | -To download access log report to CSV or TXT format                       |
| 9. Capture Fingerprint   | - To capture fingerprint images (for review purpose).                     |
| 10.Remote Door Open      | - To open the door using the web interface.                               |
| 11.Reboot                | - To reboot the unit remotely.  |

The above is a brief overview of what the features on the left panel are, in the next section, you will be able to understand for more details about what each function does, and how to set up your ACTAtek3™ and manage the system accordingly.

## 8.2. User Administration

### 8.2.1. Attendance Report

Under User Administration, select the option listed as "Attendance Report", by clicking this following screen should be displayed:



**Attendance Report**

**Search Options**

Name:  ID:

User:

Period:  From:  To:

Time:  or  Department:

Others:

Fill in the form to filter the report, or leave it blank for a full report

**Export**

Format:

Reports 1 of 1 << < 1 > >>

	User ID	Name	Date	Weekday	In Out	Total Working Hours
1	168	David Wong	2013/08/13	Tuesday	08:58:16 16:58:40	8.01

Reports 1 of 1 << < 1 > >>

This report will give you a summary of the IN/OUT of any given user (up to 10 sets of IN/OUT).

There are 4 different searching options available to view the Attendance Report which includes "Name", "User ID", "Fixed Period" or "Specific Range of Date" and "Department".

The information that can be viewed as "User ID" followed by "Name", "Date", "Day of Weekday", "IN/OUT Time" and "Total Working Hours".

You get an overview of the Total Hours worked by any given employee on any day, provided the event logs haven't been deleted. This information can then be exported to CSV or TXT files.

## Daily report

Under User Administration, select the option listed as "Daily Report", by clicking this following screen should be displayed:

**ACTAtek** The worldwide leader in Web based technologies.

**Terminal**

- Log Off
- Terminal Status

**User Administration**

- Attendance Report
- Daily Report**
- View Event Log
- Add Event Log
- View User List
- Add New User
- Departments
- User Messages

**Access Control**

- Access Groups
- Triggers
- Holidays Setting

**Terminal Settings**

- Terminal Setup
- Authentication/Log Setup
- Terminal List
- Door Open

### Daily Report

**Search Options**

Name:  ID:

User:

Period:  or From:  To:

Time:  or Department:

Others:

Fill in the form to filter the report, or leave it blank for a full report

**Export**

Format:

Report 1 of 1

	User ID	Name	Date	Weekday	First In	Last Out	Inside
1	168	David Wong	2013/08/13	Tuesday	08:58:16	16:58:40	*

Report 1 of 1

This report will give you a summary of the First IN and Last OUT of any given user ,and the user's status.(Inside or not)

There are 4 different searching options available to view the Attendance Report which includes "Name", "User ID", "Fixed Period" or "Specific Range of Date" and "Department".

The information that can be viewed as "User ID" followed by "Name", "Date", "Day of Weekday", "First IN" , "Last OUT" and "Inside"(the user's status).

You get an overview of employee's First IN and Last OUT event logs on any day. This information can then be exported to CSV or TXT files, and was very useful for the 3<sup>d</sup> party HRMS or Payroll company to import the data into their system.

### 8.2.2. View Event Log

Under User Administration, the first option listed is “View Event Log”, by clicking this following screen should be displayed:

ACTAtek The worldwide leader in Web based technologies.

**Terminal**

- Log Off
- Terminal Status

**User Administration**

- Attendance Report
- Daily Report
- View Event Log
- Add Event Log
- View User List
- Add New User
- Departments
- User Messages

**Access Control**

- Access Groups
- Triggers
- Holidays Setting

**Terminal Settings**

- Terminal Setup
- Authentication/Log Setup
- Terminal List
- Door Open

### Event Log

**Search Options**

Name:  ID:

User:

Period:  Today  or  From:  2013  8  To:  2013  8

Department:  Event:

Others:

Fill in the form to filter the report, or leave it blank for a full report

Event 1-2 of 2 << < 1 > >>

	User ID	Name	Department	Date Time	Event	Terminal	Captured Image	Remark
1	168	David Wong	General	2013/08/13 16:58:40	OUT	ACTAtek	<a href="#">View Image</a>	#FP#
2	168	David Wong	General	2013/08/13 08:58:16	IN	ACTAtek	<a href="#">View Image</a>	#FP#

Event 1-2 of 2 << < 1 > >>

There are 6 different searching options available to view the Event Log which include “User Name”, “User ID”, “Department”, “Event”, “Period” or specify the “Dates To & From”.

The information listed by an event log is “User ID” followed by “Name”, “Department”, “Date & Time”, “Event”, “Terminal”, “Capture Image” and “Remark”.

The Remark column shows how the user has gotten access by PIN, Fingerprint or Smartcard. It shows the login ID for PIN, the Smartcard number by card. If the Log Unauthorized Event is enabled, you can see which method the unknown user tried to gain access whether it is smartcard, fingerprint or PIN.

To sort the list, click on the column header, for instance, to sort by Event, click on the column header “Event”, which is in blue, and the list will be sorted in alphabetical order. By default, the displayed list is sorted by Date/Time.

#### 8.2.2.1. Deleting Event Logs

To delete event logs, click the drop-down menu at the bottom of the page, and you have an option to clear logs that are older than the available selection time. These are “this week”, “last week”, “this month” and “last month”.

### 8.2.3. Add Event Log

There are many times when a user forgets to clock in or clock out from their terminal. This option is especially introduced for Administrators to make the export of the data more accurate so that it can be easily handled by any payroll system without much hassle.

Only User Administrators and Super Administrators have the power to add/modify an event log, which could cause changes to the report and must be treated carefully. The following shows you how to add an event log into the system.

ACTAtek The worldwide leader in Web based technologies.

**Terminal**

- Log Off
- Terminal Status

**User Administration**

- Attendance Report
- Daily Report
- View Event Log
- Add Event Log
- View User List
- Add New User
- Departments
- User Messages

**Access Control**

- Access Groups
- Triggers
- Holidays Setting

**Add Event Log**

Event Log Details

User ID:

Date and Time: 2013  8  13  (yyyy/mm/dd) 17  3  23  (hh:mm:ss)

Event:

Terminal:

☒ Disable ☐ Enable

Custom Remark: Message:

Character(s) Left:

Select “Add Event Log” under User Administration from the left of your screen, and the above screen should be displayed.

Enter the Employee ID for whom the event is being added, and enter the Date & Time in yyyy/mm/dd & hh:mm:ss formats. Select the Event & Terminal being added from the drop down menus. Select the radio button “Enable” to add a remark to this event log entry (optional).

Click “Add” to append the event to your unit or “Reset” to cancel any changes made. Once Add is successfully completed, the confirmation message “Add Event Log Successful” should appear in red color.

## 8.2.4. View User List

To view the users already enrolled in the system, either by fingerprint or smart card or PIN, click on “View User List” under User Administration from the left column.

ACTAtek The worldwide leader in Web based technologies.

**User List**

Last Name First Name User ID Department Access Group Search

Export Format TXT Export

\*SMC Type: M:Mifare Card C:Contact Card L:Legic Card B:Barcode Hp:HID Prox Card Hl:HID IClass Card E:EM Card Fe:FeliCa Card Hb:Hid CEPAS Card

User 1-8 of 8

	User ID	Last Name	First Name	Other Name	Active	FP	*SMC	PSW	A/M	A/M GROUP	IN/OUT
<input type="checkbox"/>	1	089	--	--	--	•	•	•	•	•	--
<input type="checkbox"/>	2	189	--	--	--	•	•	•	•	•	--
<input type="checkbox"/>	3	896	--	--	--	•	•	•	•	•	--
<input type="checkbox"/>	4	123	--	--	--	•	•	•	•	•	--
<input type="checkbox"/>	5	888	--	--	--	•	•	•	•	•	IN
<input type="checkbox"/>	6	147	--	--	--	•	•	•	•	•	IN
<input type="checkbox"/>	7	168	--	--	--	•	•	•	•	•	IN
<input type="checkbox"/>	8	A999	--	--	--	•	•	•	•	•	--

Select All Deselect All

User 1-8 of 8

Deactivate Activate Enable Automatch Disable Automatch Delete

There are 5 different searching options available to view the User List which include “Last Name”, “First Name”, “User ID”, “Department” or “Access Group”.

The information listed in a user entry is “User ID” followed by “Last Name”, “First Name”, “Other Name”, “Active”, “FP”, “SMC”, “PSW”, “A/M”, “A/M Group”, and “IN/OUT”.

Description of Information displayed:

Feature	Description
i. Active	The Status of the User: Black –Active , Grey - Inactive
ii. FP	Whether Fingerprint is an available authentication option.
iii. SMC	Whether Smart Card is an available authentication option.
iv. PSW	Whether Password / PIN is an available authentication option.
v. A/M	Whether Auto-match is an available authentication option.
vi. A/M Group	Whether Auto-match Group is an available authentication option.
vii. IN/OUT	Whether the user is currently In or Out of Premises.

“Export”: You can export a list of registered users and their status into TXT/CSV file format.

### 8.2.4.1. To sort:

To sort the list, click on the column header, for instance, to sort by Last Name, click on the column header "Last Name", which is in blue, and the list will be sorted in alphabetical order. By default, the displayed list is sorted by ID.

### 8.2.4.2. To Deactivate / Activate /Enable or Disable Automatch / Delete Users:

To delete users from the system, you can select the checkboxes on the left of the ID under User List. If all the users need to be deactivated/deleted/activated, click the "Select All" to check ALL boxes. To cancel the selection, click on "Deselect All". Once selected, click the respective buttons at the bottom of the page, as shown below.

ACTAtek The worldwide leader in Web based technologies.

**User List**

Last Name First Name User ID Department Access Group Search

Export  
Format: TXT Export

\*SMC Type: M:Mifare Card C:Contact Card L:Legic Card B:Barcode Hp:HID Prox Card Hi:HID IClass Card E:EM Card Fe:FeliCa Card Hb:Hid CEPAS Card

User 1-8 of 8 << < 1 > >>

	User ID	Last Name	First Name	Other Name	Active	FP	*SMC	PSW	A/M	A/M GROUP	IN/OUT
<input type="checkbox"/>	1	089	--	--	--	•	•	•	•	•	--
<input type="checkbox"/>	2	189	--	--	--	•	•	•	•	•	--
<input type="checkbox"/>	3	896	--	--	--	•	•	•	•	•	--
<input type="checkbox"/>	4	123	--	--	--	•	•	•	•	•	--
<input type="checkbox"/>	5	888	--	--	--	•	•	•	•	•	IN
<input type="checkbox"/>	6	147	--	--	--	•	•	•	•	•	IN
<input type="checkbox"/>	7	168	--	--	--	•	•	•	•	•	IN
<input type="checkbox"/>	8	A999	--	--	--	•	•	•	•	•	--

Select All | Deselect All

User 1-8 of 8 << < 1 > >>

Deactivate Activate Enable Automatch Disable Automatch Delete

Once deleted, the user will no longer be in the system and all their relevant information will be removed from the system, so make sure you really want to delete them before carrying out the process.

Deactivation can take place if users or employees are no longer required to use the system for a period of time to prevent unauthorized access to the premises. Once you deactivate a user, the dot in the column "Active" will appear grey.

To activate them again, check the box next to their ID and click "Activate". This is a lot more flexible than deleting a user, since it will keep the user in the system but just restrict access for the specified time.

*Note: Starting from Firmware 1305, you can Enable/Disable Automatch users at one batch.*

## 8.2.5. To Add New Users

There are 2 ways of adding users to the system; you can either add them directly at the web interface, or at the terminal console. We have already discussed how to add a user at the terminal console (in Section 6.2), now let us look at how to add a user directly from the web interface.

### 8.2.5.1. To Add A New User:

Click on “Add New User” from the left column under “User Administration”, the following page will be displayed:

**ACTAtek** The worldwide leader in Web based technologies.

**Terminal**

- Log Off
- Terminal Status

**User Administration**

- Attendance Report
- Daily Report
- View Event Log
- Add Event Log
- View User List
- Add New User
- Departments
- User Messages

**Access Control**

- Access Groups
- Triggers
- Holidays Setting

**Terminal Settings**

- Terminal Setup
- Authentication/Log Setup
- Terminal List
- Door Open Schedule
- Bell Schedule
- Connection Profile
- Terminal Clock
- External Devices

**Terminal**

- Cloud Storage Service
- SMS Service
- Alert Log
- Syslog
- Backup System Data
- Restore System Data
- Firmware Upgrade
- Download Report
- Capture

**Add New User**

**User Details**

User ID:

Last Name:

First Name:

Other Name:

Admin Level:

Enter Password:

Note: Please leave it blank if you don't want to change/add the password.

**Access Group**

- ☒ General/General Staff
- ☐ General/Manager
- ☐ Admin/General Staff
- ☐ Admin/Manager
- ☐ Engineer/General Staff
- ☐ Engineer/Manager
- ☐ H.R./General Staff
- ☐ H.R./Manager
- ☐ Marketing/General Staff
- ☐ Marketing/Manager
- ☐ Production/General Staff
- ☐ Production/Manager
- ☐ Sales/General Staff
- ☐ Sales/Manager

**Department**

- ☒ EMERGENCY
- ☒ General
- ☐ Admin
- ☐ Engineer
- ☐ H.R.
- ☐ Marketing

Enter the User ID, Last Name, First Name, Other Name, Admin Level and enter the password in the following field. Check the relevant boxes for the relevant Access Group, this will limit or give them access at different times or doors, depending on the configuration made.

Assign the Department for the user accordingly. Select a desired fingerprint security level which ranges from Low – Normal – High – Highest. This selection affects only to the ID match ONLY and does not affect to Automatch feature.

Select the status of the user, whether they can use Auto Match or Password, and you can set the expiry date of the user if any. After that, you can click “Add” to add the new user.

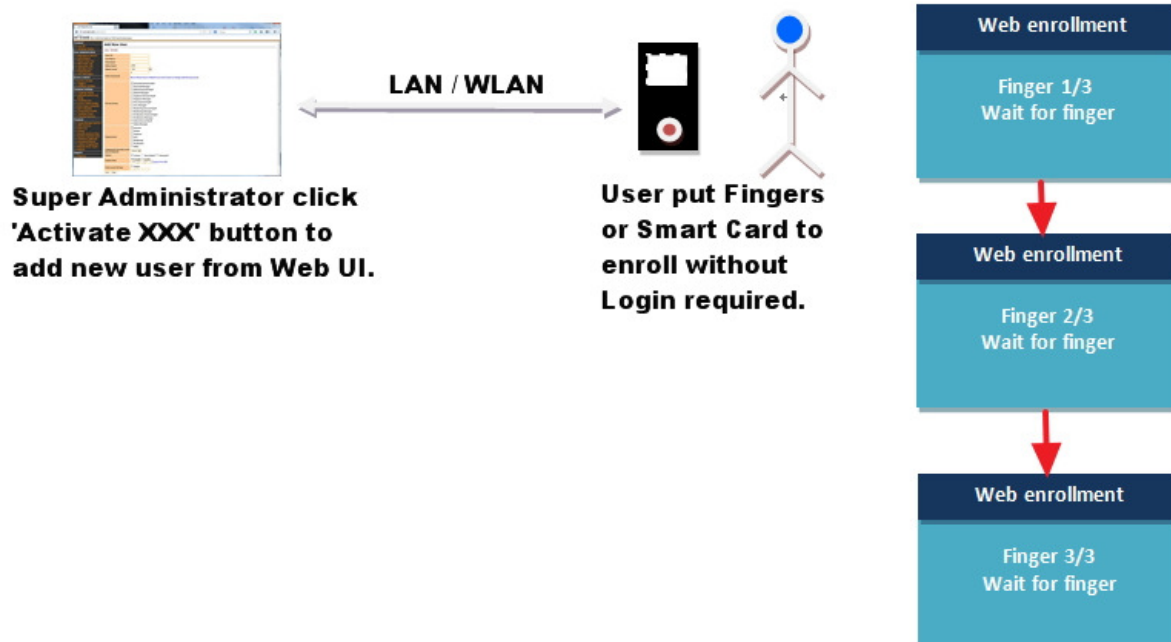
Note: Auto Match will be available when there is a FingerPrint enrolled already.

Note: First Lunch IN time (Reset) will be available when [Lunch Break Lock Out] feature was set , and F1 trigger event log was generated.

<b>Fingerprint Security Level (for ID Match)</b>	Normal <input type="button" value="v"/>
<b>Status</b>	<input checked="" type="checkbox"/> Active <input type="checkbox"/> Auto Match <input type="checkbox"/> Password
<b>Expiry Date</b>	<input checked="" type="radio"/> Disable <input type="radio"/> Enable 2013 <input type="button" value="v"/> 8 <input type="button" value="v"/> 13 <input type="button" value="v"/> (yyyy/mm/dd)
<b>First Lunch IN Time</b>	<input type="checkbox"/> Reset _/_/_ - :-
<input type="button" value="Add"/> <input type="button" value="Clear"/>	

Note: Starting from Firmware 1305, you can click “Activate Read” or “Activate Capture” from Web UI to have the remote SmartCard or FingerPrint enrollment for the new users without Login to device's console as Super Administrator. See below.

<b>SmartCard Number</b>	<input type="text"/>	<input type="button" value="Activate Read"/>
<b>Capture Fingerprint</b>	<input type="button" value="Activate Capture"/>	



## 8.2.6. Departments

This option under User Administration can be used to Add new departments, modify existing departments or delete them.

### 8.2.6.1. To Add a New Department:

Click on "Departments" under User Administration from the left column. Enter the Department Name, and description and click "Add" to append the department to the existing list.

The screenshot shows the ACTAtek web application interface. The left sidebar contains a menu with categories: Terminal, User Administration, Access Control, and Terminal Settings. Under User Administration, 'Departments' is selected. The main content area is titled 'Departments' and contains an 'Add New Department' form with fields for 'Department Name' and 'Description', and an 'Add' button. Below the form is a 'Department List' table showing 8 departments. The table has columns for 'Department Name' and 'Department Description'. The departments listed are: 1. EMERGENCY (Emergency Group), 2. General (General), 3. Admin (Administrator), 4. Engineer (Engineering), 5. H.R. (Human Resources), 6. Marketing (Marketing), 7. Production (Production), and 8. Sales (Sales). There are 'Select All' and 'Deselect All' links below the table, and 'Delete' and 'Clear' buttons at the bottom.

Department Name	Department Description
1. EMERGENCY	Emergency Group
2. General	General
3. Admin	Administrator
4. Engineer	Engineering
5. H.R.	Human Resources
6. Marketing	Marketing
7. Production	Production
8. Sales	Sales

### 8.2.6.2. To Modify Existing Departments:

Click on the Department ID, which will fill in the blanks above and make any changes, after which, clicking "Modify" would confirm the modification, or "Reset" to abort the modification.

The screenshot shows the ACTAtek web application interface. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Departments' and contains a 'Modify Department' form. The form has fields for 'Department Name' (containing 'Sales') and 'Department Description' (containing 'Sales'), and 'Modify' and 'Reset' buttons. Below the form is a 'Department List' table showing 8 departments. The table has columns for 'Department Name' and 'Department Description'. The departments listed are: 1. EMERGENCY (Emergency Group), 2. General (General), 3. Admin (Administrator), 4. Engineer (Engineering), 5. H.R. (Human Resources), 6. Marketing (Marketing), 7. Production (Production), and 8. Sales (Sales). There are 'Select All' and 'Deselect All' links below the table, and 'Delete' and 'Clear' buttons at the bottom.

Department Name	Department Description
1. EMERGENCY	Emergency Group
2. General	General
3. Admin	Administrator
4. Engineer	Engineering
5. H.R.	Human Resources
6. Marketing	Marketing
7. Production	Production
8. Sales	Sales

**8.2.6.3. To Delete Existing Departments:**

Select the check boxes of the Departments to be deleted, once selected, click “Delete” to remove them from the list of Departments, or “Clear” to abort the deletion. **Please note deleting a Department will cause its underlying Access Groups to be deleted too.**

### 8.2.7. User Messages

This option can be used to send personalized messages to individual users, who will be able to view them once they are authenticated at the ACTAtek3™ unit.

#### 8.2.7.1. To Add a New Message:

Click on “User Messages” under User Administration on the left column, the following screen should be displayed.

Enter the “User ID” and “User Message” in the User Message text box. Optionally, the message can either be displayed on the LCD screen of the ACTAtek3 or sent directly to their E-mail address, or Notify to SMS.

Click “Submit” to send the message to the user or “Reset” to abort the message. Please ensure that the message does not contain more than 25 characters per line, a maximum of 5 lines are accepted per message.

Note: You can enable “Delete the message after display once” if the user message will only be displayed one time.

#### 8.2.7.2. To delete an existing User Message:

Check the box of the relevant message, and if all need to be checked, click “Select All”, and click “Delete”. If the delete does not need to be made, click “Deselect All” to uncheck all boxes.

### 8.2.8. Admin Setting

When Login as Super Administrator, the user can configure different access rights for "Personal User" & "System Administrator" to enable or disable on 'View Event Log' or 'View/Download Reports'. See below.

**ACTAtek** The worldwide leader in Web based technologies.

Terminal	Admin Settting																			
<ul style="list-style-type: none"> <li>Log Off</li> <li>Terminal Status</li> </ul>																				
<b>User Administration</b> <ul style="list-style-type: none"> <li>Attendance Report</li> <li>Daily Report</li> <li>View Event Log</li> <li>Add Event Log</li> <li>View User List</li> <li>Add New User</li> <li>Departments</li> <li>User Messages</li> <li>Admin Setting</li> </ul>																				
<b>Access Control</b> <ul style="list-style-type: none"> <li>Access Groups</li> <li>Triggers</li> <li>Holidays Setting</li> </ul>																				
<b>Terminal Settings</b> <ul style="list-style-type: none"> <li>Terminal Setup</li> <li>Authentication/Log Setup</li> <li>Terminal List</li> <li>Door Open Schedule</li> <li>Bell Schedule</li> <li>Connection Profile</li> <li>Terminal Clock</li> <li>External Devices</li> </ul>																				
	<b>Access Rights</b> <table border="1"> <thead> <tr> <th></th> <th>Personal User</th> <th>User Administrator</th> </tr> </thead> <tbody> <tr> <td>View Attendance Report</td> <td><input checked="" type="checkbox"/></td> <td>Not available</td> </tr> <tr> <td>View EventLog</td> <td>Not available</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Attendance Report</td> <td>Not available</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Daily Report</td> <td>Not available</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Download Report</td> <td>Not available</td> <td><input checked="" type="checkbox"/></td> </tr> </tbody> </table>			Personal User	User Administrator	View Attendance Report	<input checked="" type="checkbox"/>	Not available	View EventLog	Not available	<input checked="" type="checkbox"/>	Attendance Report	Not available	<input checked="" type="checkbox"/>	Daily Report	Not available	<input checked="" type="checkbox"/>	Download Report	Not available	<input checked="" type="checkbox"/>
	Personal User	User Administrator																		
View Attendance Report	<input checked="" type="checkbox"/>	Not available																		
View EventLog	Not available	<input checked="" type="checkbox"/>																		
Attendance Report	Not available	<input checked="" type="checkbox"/>																		
Daily Report	Not available	<input checked="" type="checkbox"/>																		
Download Report	Not available	<input checked="" type="checkbox"/>																		
	<input type="button" value="Submit"/> <input type="button" value="Reset"/>																			

## 8.3. Access Control

### 8.3.1. Access Groups

An Access Group allows for users to be given standard access for the workplace. Different departments may have different access rights and some corporations have employers who are on shift duties, and may need different access levels for each shift, depending upon their time of entry and exit from the workplace. To fasten the procedure of giving access rights, it can now be done for groups, instead of individuals to simplify the process and give it more transparency. This option can only be configured by the User Administrator or the Super Administrator.

#### 8.3.1.1. To View/Delete Existing Access Groups:

Click on “Access Groups” under “Access Control” from the left column, which will display the following page:

ACTAtek The worldwide leader in Web based technologies.

**Access Groups**

Department:  Search

Access Group List

Access Group 1-14 of 14 << 1 >>

<input type="checkbox"/>	ID	Department	Access Group
<input type="checkbox"/>	1	General	General Staff
<input type="checkbox"/>	2	General	Manager
<input type="checkbox"/>	3	Admin	General Staff
<input type="checkbox"/>	4	Admin	Manager
<input type="checkbox"/>	5	Engineer	General Staff
<input type="checkbox"/>	6	Engineer	Manager
<input type="checkbox"/>	7	H.R.	General Staff
<input type="checkbox"/>	8	H.R.	Manager
<input type="checkbox"/>	9	Marketing	General Staff
<input type="checkbox"/>	10	Marketing	Manager
<input type="checkbox"/>	11	Production	General Staff
<input type="checkbox"/>	12	Production	Manager
<input type="checkbox"/>	13	Sales	General Staff
<input type="checkbox"/>	14	Sales	Manager

Select All | Deselect All

Access Group 1-14 of 14 << 1 >>

Delete

Add Access Group

Department: General

Access Group Name:

Add

You can search the access groups by Department, and click “Search”.

To Delete the Access Group(s), check the relevant box and click “Delete”, or use the “Select All” option to select ALL the access groups; or use the “Deselect All” option to clear the selection.

### 8.3.1.2. To Add a New Access Group

Under “Add Access Group”, select the relevant Department from the drop down menu and input the name of the access group being added, and click “Add”.

### 8.3.1.3. To Modify an Access Group

Click on the access group number to view the Access Group. There are two parts in this page.

ACTAtek The worldwide leader in Web based technologies.

**Terminal**

- Log Off
- Terminal Status

**User Administration**

- Attendance Report
- Daily Report
- View Event Log
- Add Event Log
- View User List
- Add New User
- Departments
- User Messages

**Access Control**

- Access Groups
- Triggers
- Holidays Setting

**Access Groups**

Modify Access Group

Access Group Name: General Staff

Department: General

Modify

Access Right ID	Terminal Name	QuickAccess
0	ACTAtek	Enable

Select All | Deselect All

Delete Access Right Add Access Right

The top part displays the Access Group Name and associate Department. This can be modified by renaming the Access Group Name and/or assigning to a different Department.

The bottom part shows a list of Access Right exist under this Access Group.

### 8.3.1.4. To Add a New Access Right

Click on “Add Access Right”. Select which terminal this access right is assigned to, and set whether Quick Access is enabled or disabled. (“Disable”: it can be used for dual access e.g. Smart Card plus FingerPrint to access the device.) Click on “Set Terminal” for proceed, as shown in the following page.

The screenshot shows the ACTAtek web interface. The left sidebar contains a menu with categories: Terminal (Log Off, Terminal Status), User Administration (Attendance Report, Daily Report, View Event Log, Add Event Log, View User List, Add New User, Departments, User Messages), and Access Control (Access Groups, Triggers, Holidays Setting). The main content area is titled 'Access Groups' and 'Add Access Right - Set Terminal'. It includes a form with the following fields: 'Access Group' (General Staff / General), 'Terminal' (ACTAtek), and 'QuickAccess' (Disable). A 'Set Terminal' button is at the bottom of the form.

On the next page select the days applicable for “Day”. Check “Always” will apply to all days.

Then select the “From” and “To” time this access right is either enabled or disabled. (Disabled access means nobody is allowed access to the unit from the relevant access group. Each user is assigned an access group when they are added into the system.)

Once the timings are assigned, select whether the access is enabled / disabled in that period, and select “Set Time” to confirm.

The screenshot shows the ACTAtek web interface. The left sidebar is the same as the previous screenshot. The main content area is titled 'Access Groups' and 'Add Access Right - Set Time'. It includes a message '[Set Time Successful]'. The form shows 'Access Group' (General Staff / General), 'Terminal' (ACTAtek), and 'QuickAccess' (Disable). Below this is a calendar grid for days 00 to 23. The grid shows days of the week (Sun, Mon, Tue, Wed, Thu, Fri, Sat, Hol) and a 'Day' column with checkboxes for 'Sun', 'Mon', 'Tue', 'Wed', 'Thu', 'Fri', 'Sat', 'Hol', and 'Everyday'. Below the grid are fields for 'From' and 'To' time (00:00 - 00:29) and a 'Set' dropdown (Enable). A 'Set Time' button is at the bottom. At the very bottom, there are two buttons: 'Submit & Create Another Access Right' and 'Submit Access Group'.

**By default all access is disabled.**

You can now either add another time setting for the same access right by select "Set Time" or create another Access right by selecting "Submit & Create another Access Right" and repeat the above steps, or confirm this access group by clicking "Submit Access Group".

### ***8.3.1.5. To Delete/ Modify Access Right***

To delete any access right, under the Modify Access Group page, check the relevant box then click "Delete". If all access rights are to be removed, click "Select All" then click Delete to remove them from the system, or click "Deselect All" to undo the selection.

To Modify the Access Right, click on access right number under "Access Right ID".

The information that can be modified includes:

- |                  |   |
|------------------|---|
| Quick Access:    | -Choose to access the device using FingerPrint or Smart Card or PIN (Quick access: Enable) or dual access (Quick access: Disable) |
| The Access Time: | -From which day and when does this Access Group is allow to access the terminal.  |

## 8.3.2. Triggers

### 8.3.2.1. To View or Modify Existing Trigger List

The “Triggers” option under Access Control shows you a number of different triggers preset into the system; this is for easy monitoring of attendance and other options. To view the list of triggers in the system, click on “Triggers” from the left column under Access Control.

To view or modify the details for the relevant trigger, click the “Trigger” on the left of the Trigger Name.

**ACTAtek** The worldwide leader in Web based technologies.

**Terminal**

- Log Off
- Terminal Status

**User Administration**

- Attendance Report
- Daily Report
- View Event Log
- Add Event Log
- View User List
- Add New User
- Departments
- User Messages

**Access Control**

- Access Groups
- Triggers
- Holidays Setting

**Terminal Settings**

- Terminal Setup
- Authentication/Log Setup
- Terminal List
- Door Open Schedule
- Bell Schedule
- Connection Profile
- Terminal Clock
- External Devices

**Terminal**

- Cloud Storage Service
- SMS Service
- Alert Log
- Syslog

## Triggers

Trigger List

Set F1 - LunchIN, F2 - LunchOut

Trigger	Trigger Name	Trigger	Trigger Name
<a href="#">IN</a>	IN	<a href="#">F20</a>	F20
<a href="#">OUT</a>	OUT	<a href="#">F21</a>	F21
<a href="#">F1</a>	F1	<a href="#">F22</a>	F22
<a href="#">F2</a>	F2	<a href="#">F23</a>	F23
<a href="#">F3</a>	F3	<a href="#">F24</a>	F24
<a href="#">F4</a>	F4	<a href="#">F25</a>	F25
<a href="#">F5</a>	F5	<a href="#">F26</a>	F26
<a href="#">F6</a>	F6	<a href="#">F27</a>	F27
<a href="#">F7</a>	F7	<a href="#">F28</a>	F28
<a href="#">F8</a>	F8	<a href="#">F29</a>	F29
<a href="#">F9</a>	F9	<a href="#">F30</a>	F30
<a href="#">F10</a>	F10	<a href="#">F31</a>	F31
<a href="#">F11</a>	F11	<a href="#">F32</a>	F32
<a href="#">F12</a>	F12	<a href="#">F33</a>	F33
<a href="#">F13</a>	F13	<a href="#">F34</a>	F34
<a href="#">F14</a>	F14	<a href="#">F35</a>	F35
<a href="#">F15</a>	F15	<a href="#">F36</a>	F36
<a href="#">F16</a>	F16	<a href="#">F37</a>	F37
<a href="#">F17</a>	F17	<a href="#">F38</a>	F38
<a href="#">F18</a>	F18	<a href="#">F39</a>	F39
<a href="#">F19</a>	F19	<a href="#">F40</a>	F40

[View Log](#) [View Log](#)

[Reset All Trigger Schedule](#) [Disable Repeat Trigger List](#)

Users can then set each terminal's trigger schedule individually.

Setting a Trigger schedule will display the respective Trigger as the default Trigger on the bottom right corner of the ACTAtek3 LCD screen, and will save the Event Log with the selected Trigger name when the user access the device.

The below following page which it will show the time settings for the trigger, grey dots stand for disabled, while the black dots stand for enabled.

**ACTAtek** The worldwide leader in Web based technologies.

**Terminal**

- Log Off
- Terminal Status

**User Administration**

- Attendance Report
- Daily Report
- View Event Log
- Add Event Log
- View User List
- Add New User
- Departments
- User Messages

**Access Control**

- Access Groups
- Triggers
- Holidays Setting

**Terminal Settings**

- Terminal Setup
- Authentication/Log Setup
- Terminal List
- Door Open Schedule
- Bell Schedule
- Connection Profile
- Terminal Clock
- External Devices

**Terminal**

- Cloud Storage Service
- SMS Service
- Alert Log
- Syslog
- Backup System Data
- Restore System Data
- Firmware Upgrade
- Download Report
- Capture Fingerprint

**Trigger Details**  
[Set Trigger Time Successful]

Trigger: F1  
Trigger Name: lunchout (Max. 8 characters)  
Enable/Disable: ☒ Enable ☐ Disable  
Modify

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

Trigger: IN  
Sun Mon Tue Wed Thu Fri Sat Hol Everyday  
Day: ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐  
From: 00:00 To: 00:28  
Set: Enable  
Set Time

To modify the time settings & other information for the relevant trigger displayed, The information to be modified includes:

- Trigger Name - Display name for the Trigger.
- Day - The days for the setting to be adjusted.
- From (Time) - Select the onset of this trigger.
- To (Time) - Select the end of this trigger.
- Set - Set whether to enable or disable it.

To confirm the change, click "Modify" to set the Trigger Name and "Set Time" to update the schedule.

### 8.3.3. Holidays Settings

The Holidays Settings option is for companies that have unique access rights or options for those days. Holiday setup can be done from "Access Rights Control" by clicking on "Holidays", which will show the following screen:

ACTAtek The worldwide leader in Web based technologies.

**Holidays**

Company Holidays(yyyy/mm/dd)  
[ 2013/12/25 ] [ 2013/12/31 ]  
Click to remove date from holiday list

<<2012 Select Month: Dec, 2013 2014>>

**2013 Dec**

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	31				

Click to add date to holiday list

Date of Holiday(yyyy/mm/dd):  Add

Copyright © 2001-2011 by ACTAtek Pte Ltd.

To add a new holiday, either click on the calendar to find the dates to add. Or type out the date in yyyy/mm/dd format and click "Add".

To remove holidays, click on the holidays already in the list and they will be automatically removed from the system.

## 8.4. Terminal Settings

### 8.4.1. Terminal Setup

To make any system configuration changes to the system, click on Terminal Setup under "Terminal Settings" from the left column. All system changes that are technically related will be available from this option for the network and super administrator.

**ACTAtek** The worldwide leader in Web based technologies.

**Terminal**

- Log Off
- Terminal Status

**User Administration**

- Attendance Report
- Daily Report
- View Event Log
- Add Event Log
- View User List
- Add New User
- Departments
- User Messages
- Admin Setting

**Access Control**

- Access Groups
- Triggers
- Holidays Setting

**Terminal Settings**

- Terminal Setup
- Authentication/Log Setup
- Terminal List
- Door Open Schedule
- Bell Schedule
- Connection Profile
- Terminal Clock
- External Devices

**Terminal**

- Cloud Storage Service
- SMS Service
- Alert Log
- Syslog
- Backup System Data
- Restore System Data
- Firmware Upgrade
- Download Report
- Capture Fingerprint
- Capture Picture
- Remote Door Open
- Reboot

### Terminal Setup

#### Network Settings

Terminal ID	0
Serial Number	00111DA040C3
Terminal Description	ACTAtek
IP Address	<input type="radio"/> DHCP <input checked="" type="radio"/> Static IP Address: 192.168.1.200
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
DNS Server	192.168.1.254

#### Fingerprint Related Setting

Security Level (for Automatch)	Normal
--------------------------------	--------

#### Smart Card Related Setting

Parity Error detection	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
------------------------	---

#### Console Display Timeout Settings

Welcome Message Timeout	1 sec
Console Display Timeout	30 sec
Console Clock Format	<input type="radio"/> 12 hours <input checked="" type="radio"/> 24 hours

#### Wiegand Configuration

Wiegand Type	Disable
Access Method	Finger Print, Password
Wiegand Output Format	User ID + Facility Code
User Facility Code (FC)	1 (1 - 255)

The options that can be changed include Network Settings, Fingerprint Matching Setting & Miscellaneous Setting:

Terminal Description	- The Description of the terminal
IP Address	- The IP Address of the terminal (Dynamic or Static)
Subnet Mask	-If enable DHCP, it will be automatically entered.
Default Gateway	-If enable DHCP, it will be automatically entered..
DNS Server	- If enable DHCP, it will be automatically entered.

Security Level (for Automatch)	- The Fingerprint Security level for the system. Lower the level for higher and successful matching rate.
Smart Card Related Setting	- Choose to Enable or Disable Parity Error detection for HID prox. cards.
Console Display Timeout Settings	-You can select from 1sec to 3 sec.
- Welcome Message Timeout	-You can select from 30 sec to 1 hour.
- Console Display Timeout	
Wiegand Output	- This option is to enable Wiegand output from the unit to the external I/O board or on-board Wiegand output.
Terminal Mode	- <b>Standalone</b> : the device will work with previous ACTA2 SOAP/API. - <b>Access Manager</b> : the device is able to register with the Access Manager.
Job Code	-Disable / Enable. <b>(See Appendix A.)</b>
Door SW Mode	-Choose Door Switch or Door Sense
Door Strike 1 Option	- Setting for Door Strike to open door.
-Emergency Mode	-For users who were assigned to EMERGENCY department can open door.
	<b>(See Appendix B.)</b>
-Relay Delay	- This will keep the door open for the seconds specified.
Door Strike 2 - Door Strike 1 Clone	- To set Door Strike behave as Door Strike1
Door Strike 2 – Access Denied	- To be triggered when the login is access denied.
Door Strike 2 - Bell Schedule	- To enable the Bell schedule option.
Door Strike 2 – Active Alarm	- Trigger the Alarm connector when door opened more than 30 seconds
<i>(*Door Strike2 is required to connect to external I/O board .)</i>	
Network Camera	- To enable external network camera during Remote Door Open.
Language	- This option lets you select between various languages.
Webserver Port	- Specify other port to use for the webserver.
Allowed IP	- Restrict IP address(es) to access this web interface.
2-digit Duress Code	- Numeric code use as duress code. This is used as prefix in the user password.
SMTP Server	- SMTP Server for outgoing mail sent by the unit. <b>(See Appendix C.)</b>

## 8.4.2. Authentication/Log Setup

ACTAtek The worldwide leader in Web based technologies.

**Authentication/Log Setup**

**Log Setup**

Log Event: ☐ Disable ☒ Enable User Log

Log Size: 10 k

Log Unauthorized Event: ☒ Disable ☐ Enable

Accept Unregistered Smartcard: ☒ Disable ☐ Enable

Photo Option for Log: ☒ Authorized Event ☒ Unauthorized Event

**Authentication**

☒ Disable

☐ Auto IN/OUT ☐ Auto Reset IN/OUT

☐ Reject Repeated Event in  sec (1 - 86400)

☐ Anti-passback (Note: Anti-pass back will be reset at 00.00 hours)

☐ Lunch Break Lock Out  min (1 - 120)

Submit Reset

### Log Setup

-Log Event: To choose to disable or enable event logs generated at the device.

*Note: Starting from Firmware 1305, the user can choose to enable logs for 'User Log' or 'Audit Log' or both to be viewed from [View Event Log]. See below.*

**Event Log**

Search Options

Name ID

User

Period From To

Time Today or 2013 9 2013 9

Department Event

Others

Fill in the form to filter the report, or leave it blank for a full report Search

Event 1-7 of 7

User ID	Name	Department	Date Time	Event	Terminal	Captured Image	Remark
1	108	General	2013/09/04 15:37:45	IN	ACTAtek	<a href="#">View Image</a>	#FP#
2	108	General	2013/09/04 15:37:35	IN	ACTAtek	<a href="#">View Image</a>	#FP-SMC#
3	0904	General	2013/09/04 15:37:28	OUT	ACTAtek	<a href="#">View Image</a>	#FP#
4	0904	General	2013/09/04 15:37:24	IN	ACTAtek	<a href="#">View Image</a>	#FP#
5	0904	General	2013/09/04 15:37:10	OUT	ACTAtek	<a href="#">View Image</a>	#FP#
6	0904	General	2013/09/04 15:37:02	IN	ACTAtek	<a href="#">View Image</a>	#FP#
7	A999		2013/09/04 15:36:33	ADMIN LOGIN	ACTAtek		#CONSOLE Modified FP User ID:0904#

Event 1-7 of 7

-Log Size: To choose to store off-line event logs storage size.e.g.10K or 75K.

-Log Unauthorized Event: To choose to disable or enable on whether to store the unauthorized event or not.

-Accept Unregistered Smartcard: To choose to disable or enable on whether to accept and record the unregistered smart card or not.

-Photo Option for Log (Authorized Event/ Unauthorized Event): To choose whether to take a snapshot for the authorized event or unauthorized event.

**Additional Security Options (See Appendix D. for more information)**

-Auto IN/OUT: It is a feature for time attendance that allow the system assume the first authentication is IN and follow by OUT without having the user to select the function key of IN or OUT.

-Auto Rest IN/OUT: The device will reset at 2359hrs and the next authentication will be IN.

-Reject repeated event: It is a feature that the device will reject the same event within the defined time. This is prevent double scanning, especially using RFID card

-Anti-passback: It is a feature to prevent from the tail-gating .If someone did not have IN event first, he/she will not be able to access the device as OUT event.

-Lunch Break / Lock Out: It is a feature to make sure the staff takes their lunch break as the defined time period. Lunch lockout period is configurable from 1 to 120 minutes. This lockout period is the time between F1 (LunchIN) and F2 (LunchOUT). User is not granted access when he fails to meet the above conditions.

### 8.4.3. Terminal List

The “Terminal List” option under “Terminal Settings” can be used to view the list of terminals, and their respective name, type, serial number and IP Address, as shown below.

The screenshot shows the ACTAtek web interface. The browser address bar displays <http://192.168.1.100/adr>. The page title is "ACTAtek The worldwide leader in Web based technologies." The left sidebar contains a navigation menu with the following sections:

- Terminal**
  - Log Off
  - Terminal Status
- User Administration**
  - Attendance Report
  - Daily Report
  - View Event Log
  - Add Event Log
  - View User List
  - Add New User
  - Departments
  - User Messages
- Access Control**
  - Access Groups
  - Triggers
  - Job Code
  - Holidays Setting
- Terminal Settings**
  - Terminal Setup
  - Authentication/Log Setup
  - Terminal List
  - Door Open Schedule
  - Bell Schedule
  - Connection Profile
  - Terminal Clock
  - External Devices

The main content area displays the "Terminal List" section with a table containing one terminal:

No.	Description	Type	Serial No.	IP Address	Camera	Door	Last Updated To Second
1	ACTAtek	Primary	00111DA040C3	<a href="#">192.168.1.100</a>	<a href="#">Camera</a>	<a href="#">Unlock Door</a>	--

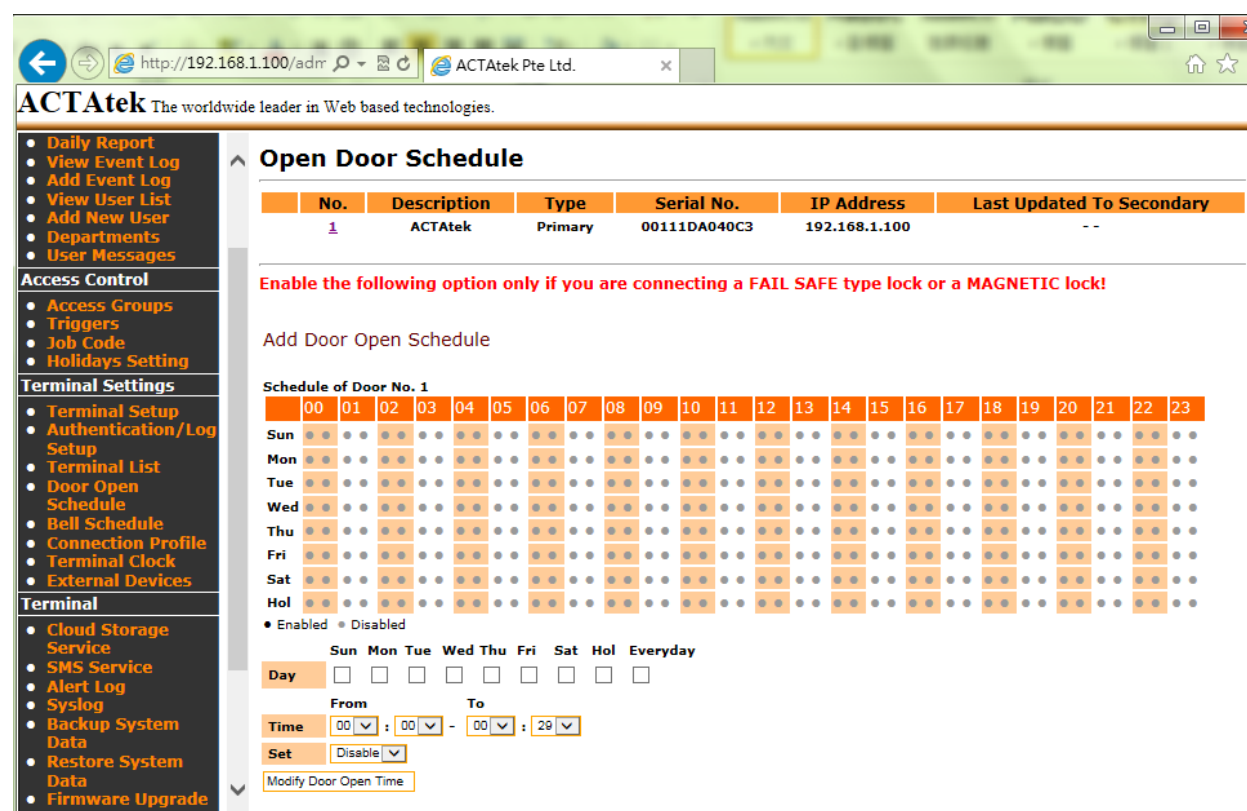
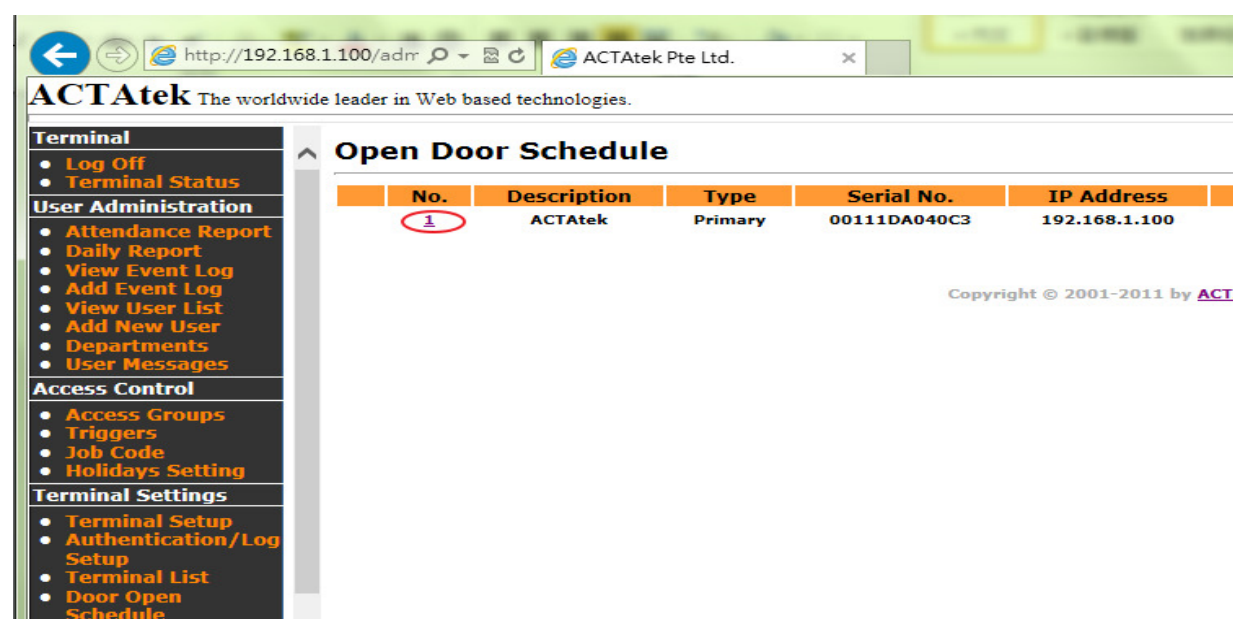
Below the Terminal List is the "Server List" section, which is currently empty with the message "No record found." and buttons for "Submit", "Delete", "Add", and "Test Modem Connection".

Copyright © 2001-2011 by ACTAtek Pte Ltd.

Under 'Server list', you can check the Event Logs sending status about the last sync. date and time with Agent ver.2's or Access Manager software's back-end database.

### 8.4.4. Door Open Schedule

The Open Door Schedule is a feature to control the open access to the door entrance. Fill out the parameters in the page to set up the time for the open access time of the door entrance.



### 8.4.5. Bell Schedule

The Bell Schedule option needs to be enabled via Door Strike 2 Option under Terminal Setup page. Once enabled, ACTAtek3 is able to trigger a bell wired to the door strike 2 connector for the scheduled time.

ACTAtek The worldwide leader in Web based technologies.

#### Bell Schedule

No.	Description	Type	Serial No.	IP Address	Bell Status	Last Up
1	ACTAtek	Primary	00111DA040C3	192.168.1.100	<a href="#">Enable</a>	

Copyright © 2001-2011 by [ACTAtek Pte Ltd.](#)

ACTAtek The worldwide leader in Web based technologies.

#### Bell Schedule

No.	Description	Type	Serial No.	IP Address	Bell Status
1	ACTAtek	Primary	00111DA040C3	192.168.1.100	<a href="#">Enable</a>

Add Bell Schedule

Bell Schedule of Door No. 1

	Day	Time	Bell	Buzzer	Duration (s)
<input type="checkbox"/>	1 Mon	12:00	ON	OFF	5
<input type="checkbox"/>	2 Tue	12:00	ON	OFF	5
<input type="checkbox"/>	3 Wed	12:00	ON	OFF	5
<input type="checkbox"/>	4 Thu	12:00	ON	OFF	5
<input type="checkbox"/>	5 Fri	12:00	ON	OFF	5

[Delete](#)

Sun Mon Tue Wed Thu Fri Sat Hol Everyday

Day ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐

Time  :

Set

Duration

[Modify Bell Schedule](#)

### 8.4.6. Connection Profile

- Reserved for the Agent configuration

### 8.4.7. Terminal Clock

The "Terminal Clock" can be modified according to the region you are in. It is extremely useful to have a correct timing for all time attendance purposes or for reporting purposes since that's the time the system will record for any access.

**ACTAtek** The worldwide leader in Web based technologies.

**Terminal Clock**  
[Set Terminal Clock Successful: Current Time - Wed Aug 14 10:08:35 2013 ]

Date: 2013/08/14 (yyyy/mm/dd)  
Time: 10:08:42 (hh:mm:ss)  
New Date: (yyyy/mm/dd)  
New Time: (hh:mm:ss)

Auto Adjust: ☐ On ☒ Off  
"On" - Automatically use your PC date/time to adjust  
"Off" - Manually type in the date/time

Set Time

Time Zone: (GMT +08:00:00) Singapore

☐ Modify

DST Setting

	Julian date	Month	week	day	Set time
Starting		--	--	--	--
Ending		--	--	--	--

☐ Enable SNTP

Server Name:   
Note: You must set the time zone correctly in order to synchronize with an SNTP server.

Set

If the SNTP (Time server) is enabled, then the ACTAtek3™ will sync. its time with SNTP server each 3 hours.

*Note: Starting from Firmware 1305, the device will automatically re-sync. the Terminal Clock with SNTP server after each reboot if SNTP was enable before.*

If the SNTP is disabled, the ACTAtek3™ will either have to follow the time on the PC or a time can be set for the device according to the local time settings.

To let ACTAtek3™ to follow the time on the PC, select "On" for Auto Adjust. To disable this auto adjust, select "Off" and the time setting will be available for users to input the "New Date" and "New Time". Click 'Set Time' to set the device's date/time after "Auto Adjust" finished.

Besides, please select the correct Time Zone where the device was installed at which region.

Click "Set" to save any modifications made.

### 8.4.8. External Devices

If ACTA3 was connected to the external I/O board, you can see the connection status at external devices page. *(Note: Starting from Firmware 1305, ACTA3 device will automatically detect the external I/O board once powered on and connected.)*

ACTAtek The worldwide leader in Web based technologies.

**External Devices**

Add New External Reader

External Reader Interface

RS485

Reader Type	Reader Address	Reader Description	Trigger	Ignore Quick Access	Baud Rate	External Secured
Mifare	1		IN	<input type="checkbox"/>	9600	<input type="checkbox"/>

Add

External Reader List

	Reader Type	Reader Address	Trigger	Ignore Quick Access	Baud Rate	External Secured Relay	FW Vers
Select All   Deselect All							

Total 0 Readers

Delete Clear

External Secured Relay List

Relay Address
1

Total 1 Relays

External IO Board

[No External I/O Board connected]

Refresh

Copyright © 2001-2011 by ACTAtek Pte Ltd.

### 8.4.9. Cloud Storage Service

-See "Appendix E. Cloud Storage Service" for more information.

### 8.4.10. Short Message Service(SMS)

-See "Appendix F. Short Message Service (SMS)" for more information.

### 8.4.11. Alert Log Settings

You can configure the alert log settings so that the device will be able to send the system's alert event log to the administrator via E-mail or SMS. See below.

**Alert Log Settings**

Administrator's Email Address:

Administrator's SMS No:

NO.	Type	Email	SMS
1	Door is opened more than 30S	<input type="checkbox"/>	<input type="checkbox"/>
2	Bottom case is detached	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	Primary is offline	<input type="checkbox"/>	<input type="checkbox"/>
4	Duress access	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Copyright © 2001

### 8.4.12. Alert Log

You can configure the remote syslog settings to store the device's system logs to the remote server. See below.

**Remote Syslog Settings**

Remote Syslog: ☒ Disable ☐ Enable

Syslog Server IP Address:

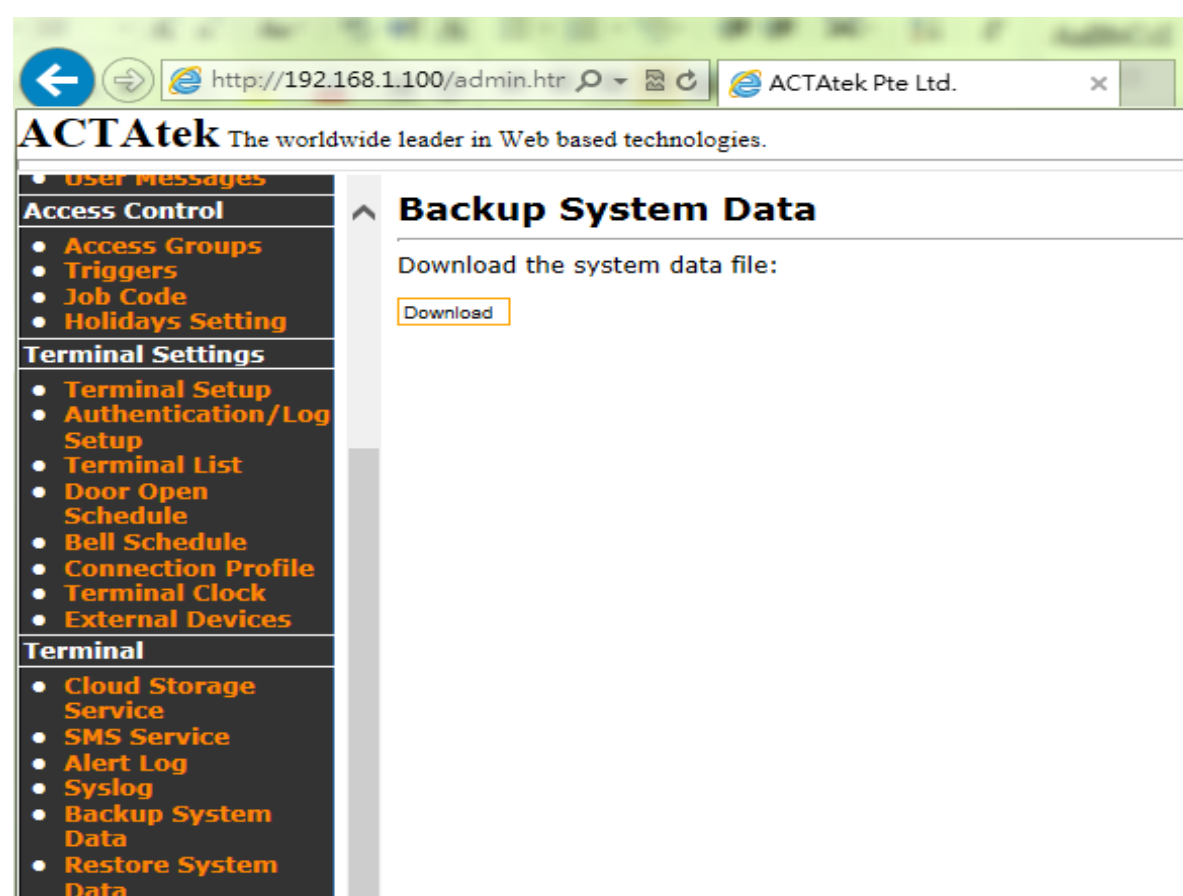
Copyright © 2001

### 8.4.13. Backup System Data

Backing up is an essential part of any system. It can provide the added security and flexibility that is needed for these devices.

With the Backup System Data feature, the system's configuration files can be saved, so as the user data. In general speaking, the user information, event logs, access group, and triggers will be saved during the backup. In that case, it could help the units share the configuration with different devices in the network, or rollback to a previous setting when something goes wrong with the system.

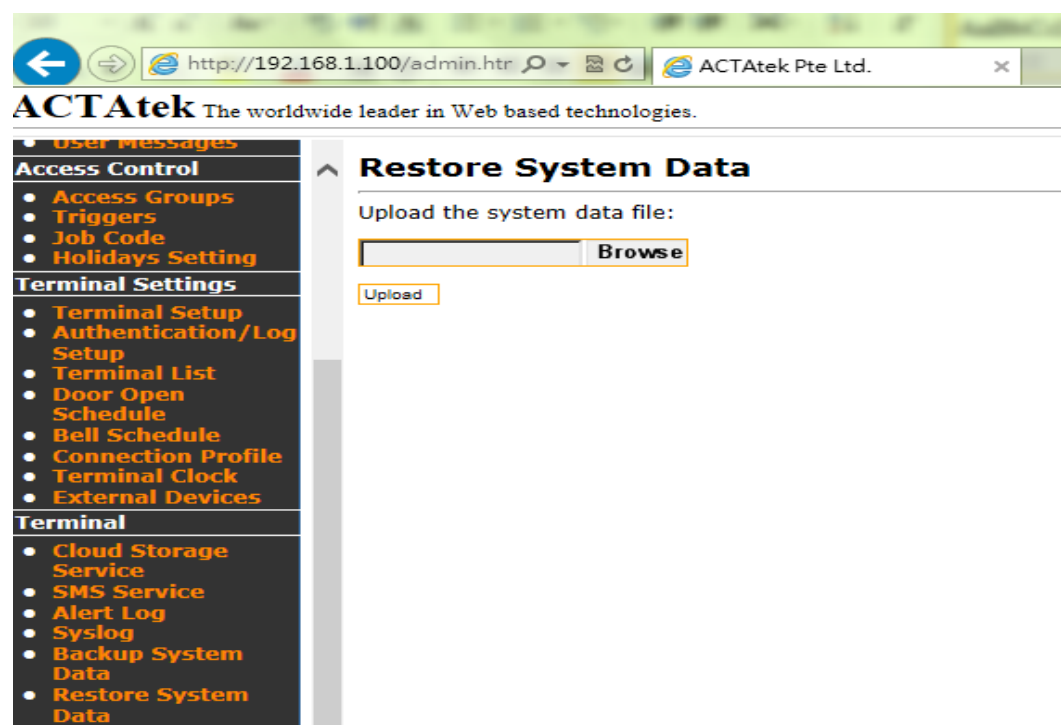
To backup the system configuration, click on "Backup System Data" under Tools from the left column of options.



Once selected, click "Download" to download the data on to the PC. The system will then prompt to save the file in the PC, click on the specified location and save the file.

#### 8.4.14. *Restore System Data*

If the device may have some issues, and required to restore, you can click “Restore System Data” option under Terminal in the left column.



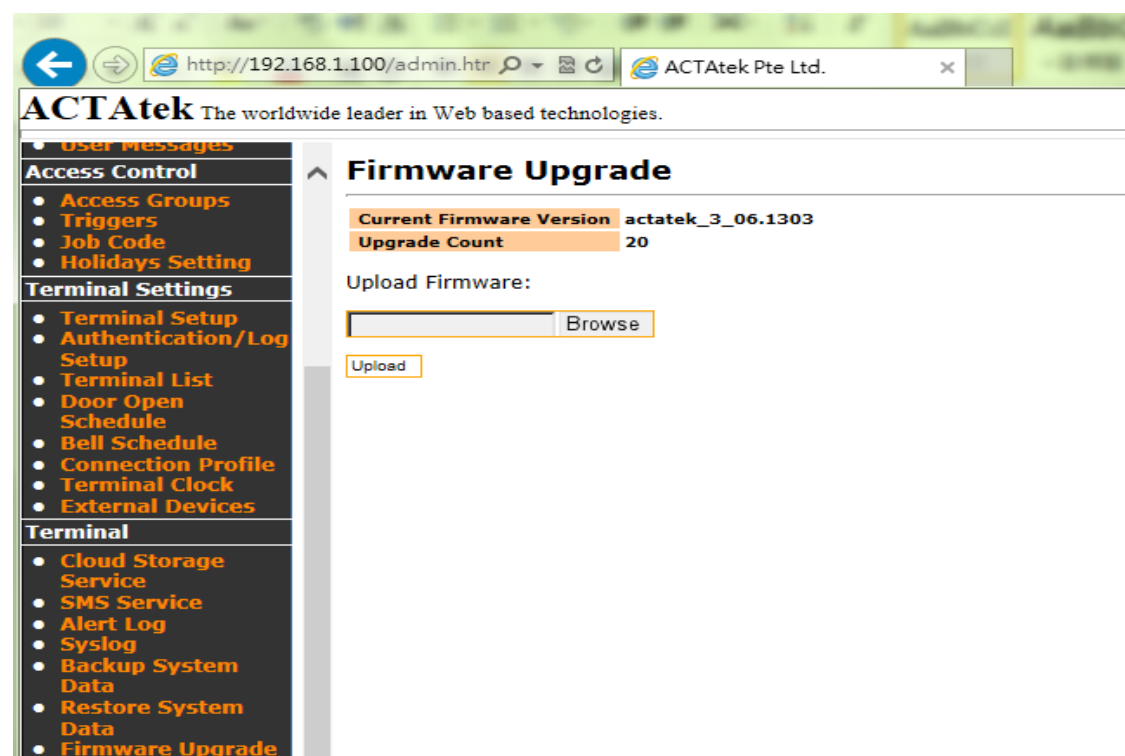
Click “Browse” to locate the specified and previous backup system file, once located, click “Open”.

Then click “Upload” to upload the file back into the system for the previous configuration to take place.

### 8.4.15. Firmware Upgrade

Firmware releases will be carried out on a regular basis. ACTAtek R&D team will continue to add new features to ACTAtek3, and provide the download links of the latest firmware for our clients to download.

To upgrade your unit with the latest firmware, click on “Firmware Upgrade” from the left column under “Terminal”.



Click “Browse” to locate the firmware (once downloaded to your machine from our website). Click “Open” once the file has been located, and “Upload” to upload it to your system. You will then be prompted to upgrade your system, this should take a couple of minutes. Once upgraded, please do reboot the unit to take effect the new firmware.

Also from this page, the current firmware version can be seen, and the upgrade count is also available to show you how many times the system has been upgraded, for your reference purposes. Once upload is clicked, the system will install the new firmware and your system will reboot automatically to let the new changes take effect. After the device finished Firmware upgrade, you can click ‘Log Off’ and re-Login to the device’s Web UI to check the ‘Terminal Status’ page.

### 8.4.16. Download Report

The Download Report option allows for easy download of attendance reports of employees in CSV or TXT format.

Reports can be downloaded by various different options, as shown below.

The screenshot displays the 'Download Report' page in the ACTAtek web application. The browser address bar shows 'http://192.168.1.100/admin.htr'. The page title is 'ACTAtek The worldwide leader in Web based technologies.' The sidebar on the left contains navigation links under 'Access Control', 'Terminal Settings', and 'Terminal'. The main content area is titled 'Download Report' and features a 'Search Options' section with the following fields:

- User:** Name (text input), ID (text input)
- Time:** Period (Today, dropdown), or (radio button), From (2013, 8, dropdown), To (2013, 8, dropdown)
- Department:** (dropdown)
- Event:** (dropdown)
- Format:** Report (TXT, dropdown)
- Download:** (button)

Below the form, it states: 'Fill in the form to filter the report, or leave it blank for a full report'. The footer of the page reads: 'Copyright © 2001-2011 by ACTAtek Pte Ltd.'

Reports can either be downloaded by:

User Name  
 User ID  
 Department  
 Period  
 From/To (Date yy/mm/dd)  
 Event  
 Format – CSV or TXT

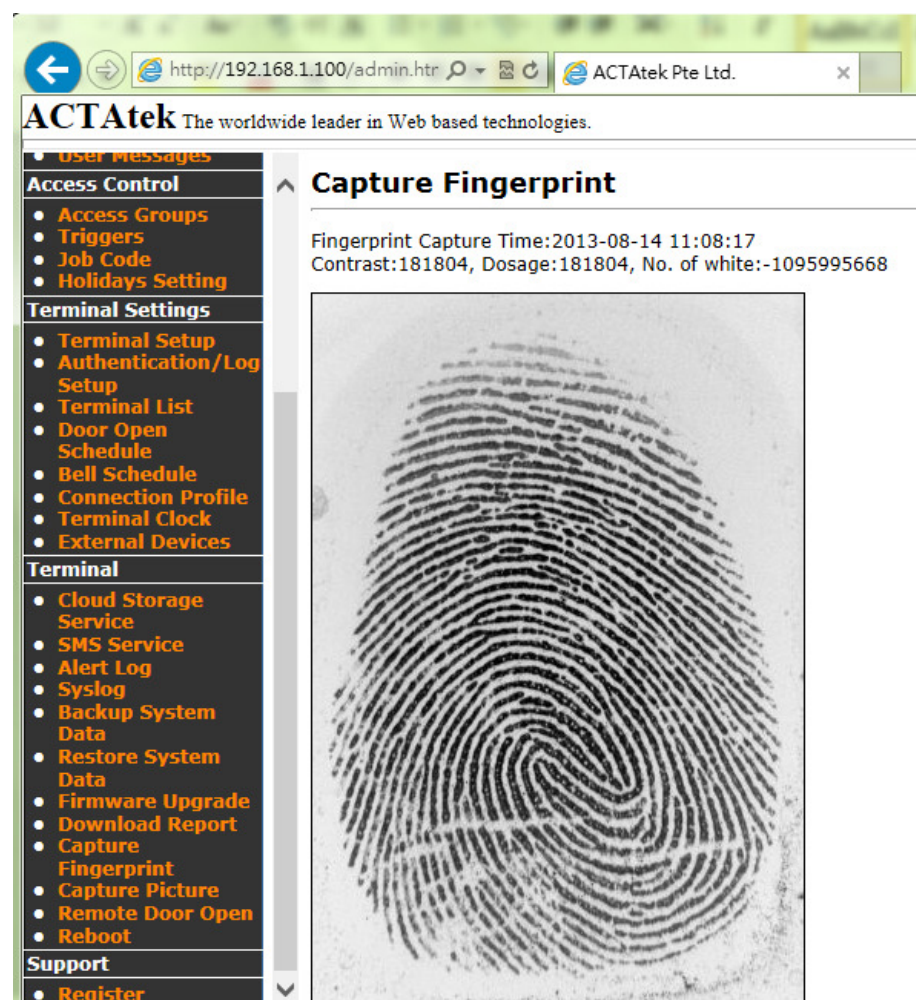
Click "Download" for the report to be downloaded to your system for payroll or other management purposes.

### 8.4.17. Capture Fingerprint

The ACTAtek3™ can capture fingerprint in real time and help in analysis of why certain fingerprints are being rejected by the unit or what is causing the rejection. This option helps the technicians better understand the fingerprint issues and what they can do to improve readings.

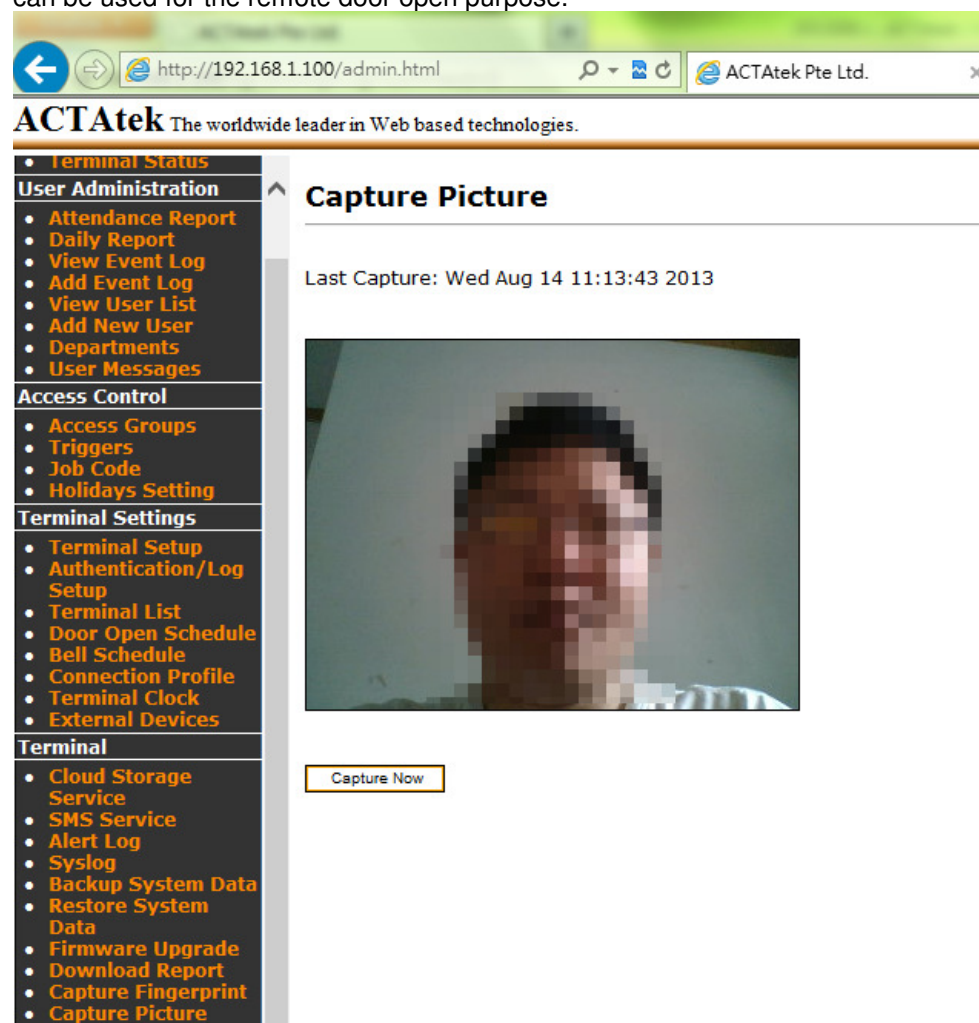
This image is captured via the terminal menu under “User Management” --> “Capture Fingerprint”. Once the fingerprint is captured, it can be viewed via the web interface, as shown below.

These images should only be used for analysis purposes, and ACTAtek is not liable for any mis-use of these images, please also note that all fingerprint data collected can only be used for scanner analysis with no other purposes.



### 8.4.18. Capture Picture

You can use this feature to take a picture for the staff's employee photo or the taken picture can be used for the remote door open purpose.

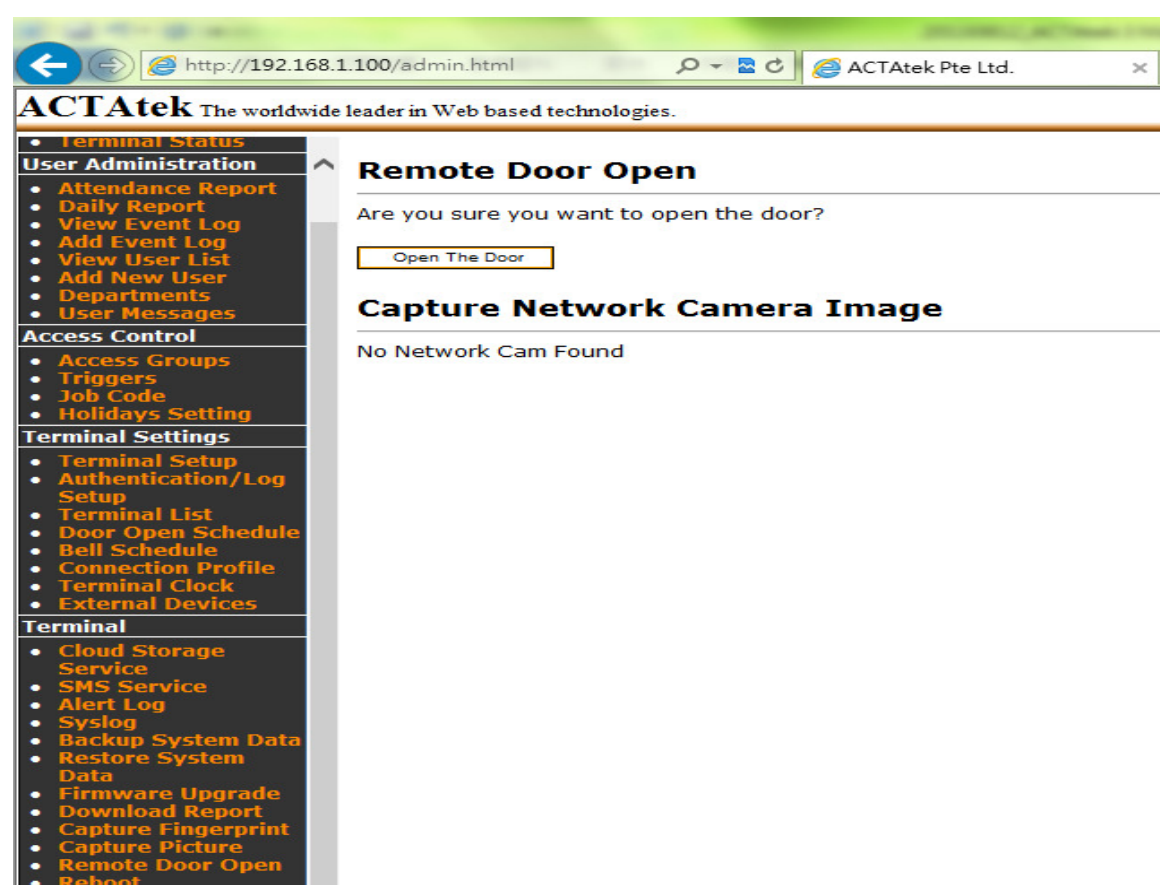


### 8.4.19. Remote Door Open

Most organizations or corporations or even small business have visitors coming in and out for meetings, or to drop parcels, etc. Those visitors are not enrolled in the system since they are not part of the company's payroll or should not have access to the office at odd hours.

For these reasons, the Remote Door Open feature comes in handy since visitors do not need to be enrolled in the unit to gain access, but the reception or someone near a computer can simply open the door using this feature, which enhances flexibility and convenience of the system.

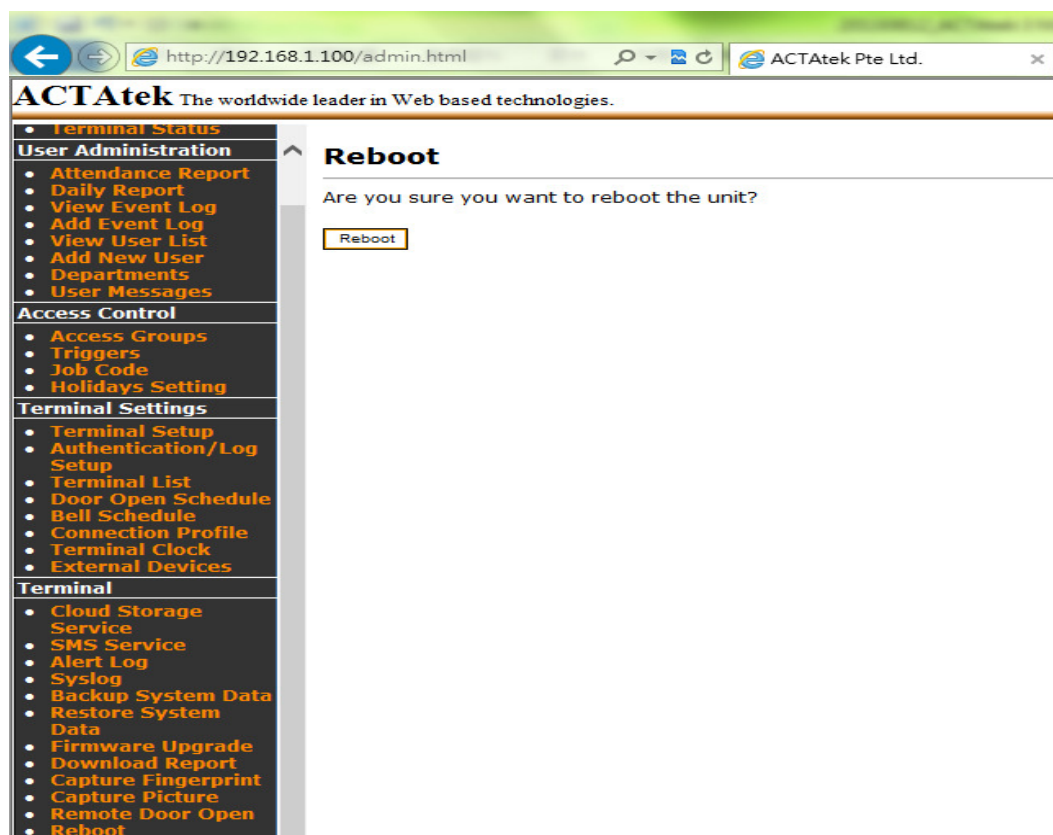
To open the door remotely from any computer, click on "Remote Door Open" under Tools, which will display the following page:



Once selected, click "Open the Door" to open the door remotely. If successful, the message "The door is opened" will be displayed.

### 8.4.20. Reboot

To reboot the ACTAtek3 remotely, the 'Reboot' option can be selected.



Click on the 'Reboot' button to reboot the unit.

### 8.4.21. Register

You will be redirected to our support website to register the device's warranty at our support website. Please follow up the product registration steps as shown in the webpage.

## Appendix A. Job code feature

**Job code** is a new feature which allows ACTAtek to provide better capability to integrate with any third party payroll/HR programs. It is an advance idea that is extended from our existing trigger features. As before, the trigger feature from ACTAtek only supports up to 40 different descriptions of Event Logs such as IN/OUT/F1 up to F40. Now, with the new job code feature established, ACTAtek can support up to 4,500,000 different combinations of Event Log descriptions.

### 1. Enable Job Code

To enable job code, please go to Terminal Setup -> Miscellaneous -> Job code and click the button to enable the feature.

**Wiegand Configuration**

Console Display Timeout: 30 sec

Wiegand Type: Disable

Access Method: Finger Print, Password

Wiegand Output Format: User ID + Facility Code

User Facility Code (FC): 1 (1 - 255)

**Miscellaneous**

Terminal Mode: ☒ Stand Alone ☐ Access Manager

Job Code: ☐ Disable ☒ Enable

Door Strike 1 Option: ☐ Disable ☒ Access Granted ☐ Emergency Mode

Relay Delay: 3 sec (1-20)

Once it is enabled, there will be Job Code setup link popped up Access Control.

**Job Code Settings**

Job Code	Description	Enable	Action
Job Code 1	Job Code	<input type="checkbox"/>	<a href="#">View List</a>
Job Code 2	Occup. Code	<input type="checkbox"/>	<a href="#">View List</a>
Job Code 3	Customise Code	<input type="checkbox"/>	<a href="#">View List</a>

Save Undo

**Job Code**

Job Code ID	Description	Enable/Disable
<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

Add Cancel

**Job Code List**

<input type="checkbox"/>	Job Code ID	Description	Enable/Disable
<a href="#">Select All</a>   <a href="#">Deselect All</a>			
<a href="#">Delete</a>			

Under the Job Code setup page, there will be 3 tables sharing in total of 500 sets of job codes. This means if Job Code table 1 is consuming 200 sets, and Job Code table 2 is consuming 200 sets, then there will only 100 sets available for Job Code table 3.

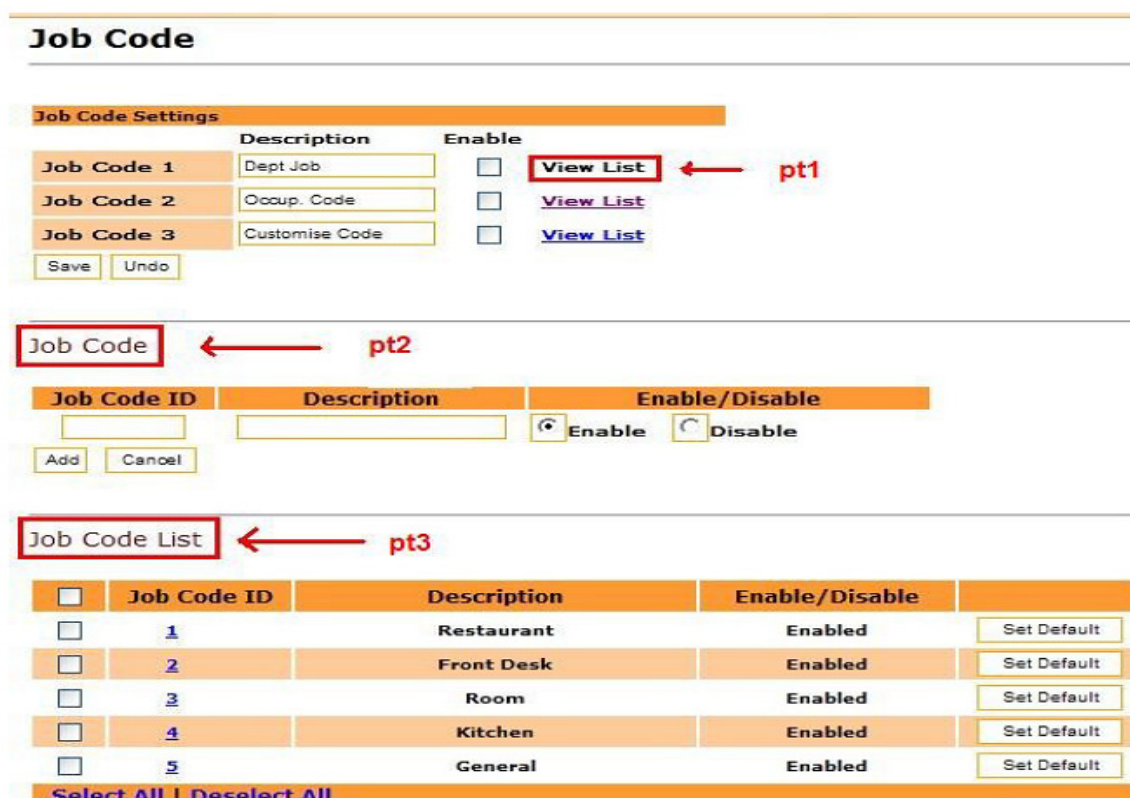
For each Job Code table, you could assign it with different descriptions. For instance, in Job code 1, you may put “Job Department” , in Job code 2, you may put “Occupations” , and etc.

It is not necessary to enable all 3 tables at the same time; you could just choose either 1 or 2 job code table to suit your setup.

To enable the job code table, simply, just click the check box beside the “View List” to enable the job code table.

## 2. Add new job code into the table

From the job code setup page, you will see each Job code table has the button called “**View List**” (See below picture, pt1). That link allows users to view the job codes stored under this table. When you click the link, you will see the Job Code List associated with that Job code table will be appeared at the bottom of the page (See below picture, pt3). As you wish to add new job code into this Job Code table, you can simple add it from the Job Code section (See below picture, pt2).



**Job Code**

---

**Job Code Settings**

	Description	Enable	
Job Code 1	Dept Job	<input type="checkbox"/>	<b>View List</b> ← pt1
Job Code 2	Occup. Code	<input type="checkbox"/>	<a href="#">View List</a>
Job Code 3	Customise Code	<input type="checkbox"/>	<a href="#">View List</a>

Save Undo

---

**Job Code** ← pt2

Job Code ID	Description	Enable/Disable
<input type="text"/>	<input type="text"/>	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

Add Cancel

---

**Job Code List** ← pt3

<input type="checkbox"/>	Job Code ID	Description	Enable/Disable	
<input type="checkbox"/>	<a href="#">1</a>	Restaurant	Enabled	<a href="#">Set Default</a>
<input type="checkbox"/>	<a href="#">2</a>	Front Desk	Enabled	<a href="#">Set Default</a>
<input type="checkbox"/>	<a href="#">3</a>	Room	Enabled	<a href="#">Set Default</a>
<input type="checkbox"/>	<a href="#">4</a>	Kitchen	Enabled	<a href="#">Set Default</a>
<input type="checkbox"/>	<a href="#">5</a>	General	Enabled	<a href="#">Set Default</a>

[Select All](#) | [Deselect All](#)

To add the new Job Code, just enter the Job Code ID (As the shown on above picture of pt2), and then mark down the Description. After that, just hit the “Add” button. Once the new job code is successfully added into the table, you will see it is being listed under the Job Code List (On pt3).

**\*\*Note**, there is an option called “Set Default” in the Job Code List. This feature provides an option that when user login and does not enter the job code, the system will automatically assign the one which has “Set Default” being activated to the user.

For example, If Job Code ID 1 (Restaurant) is being “Set Default” , then when user “A” logins without entering the job code, the system will assign him the job code, ID1 for him.

### 3. Why using Job Code?!

Under the eventlogs lists, the job code events will be recorded in the following format.

#J1(1) #J2(234) #J3(134)#

This indicates that the user logins as **job code (001) from job table 1**, **job code (234) from job table 2**, **job code (134) from job table 3**, so that such raw data in txt or CSV format could be easily integrated with any 3rd party systems and analyzed for HR, work force, or payroll purpose.

For instance, employee A999 is working for different jobs in a hotel, and those jobs are being paid in different wedges. From 10 am to 12 pm, he is being paid as a house keeper with hourly rate of \$10, and from 12 pm to 6pm, he is being paid as a front desk service with hourly rate of \$12. Without a good tracking system, the mistake may occur from day to day.

But now, with the powerful feature such Job Code Function in ACTAtek, the management team is easy to manage the human resource and generate the payroll correctly.

All they need to do is setup the job table, and ask user to punch in the job code as they are coming to work, and ACTAtek will do the rest of the jobs and ensure there no human mistakes occurring again.

## Appendix B. Emergency Mode

**Emergency mode** is designed to work with the 3<sup>rd</sup> party controller connected to ACTAtek external I/O board. The 3<sup>rd</sup> party controller will always be the master of the system to control open and close of the door via ACTAtek external I/O board's Wiegand output signal.

However, in times of failure of the 3<sup>rd</sup> party controller, the users who were associated and under emergency department will be granted to open the door during normal authentication.

### System setup:

1. System will be require to setup as connect door strike 1 of the I/O box to have a "OR" circuit to release the magnetic lock with host system (3<sup>rd</sup> party controller) as shown on figure 1.
2. Actatek device will send wiegand userid data through I/O box during device authentication to host system as shown on Figure 1 with pointer RED 1.
3. The host system will authenticate and send granted access to open the door as shown on figure 1 with pointer RED 2.
4. The Super Administrator Login to ACTAtek device's Web UI, and then goes to [Terminal Setup] to enable door strike1 option as "Emergency mode". And then go to [View User List] to click user ID to modify the user's department as "Emergency", and click [Modify] to make the changes.

After enable "Emergency mode", only users ID which was under emergency department will be able to pass the authentication to open the door strike 1 as shown on figure 1 with pointer RED 3, but other user ID will not be activate the door strike 1.

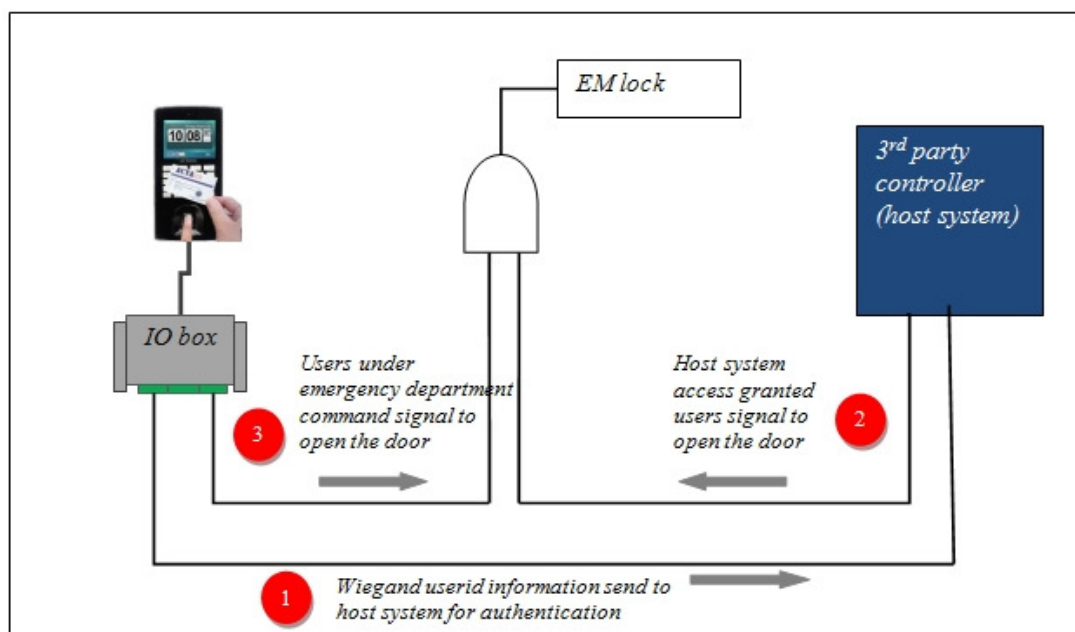


Figure1.Emergency mode

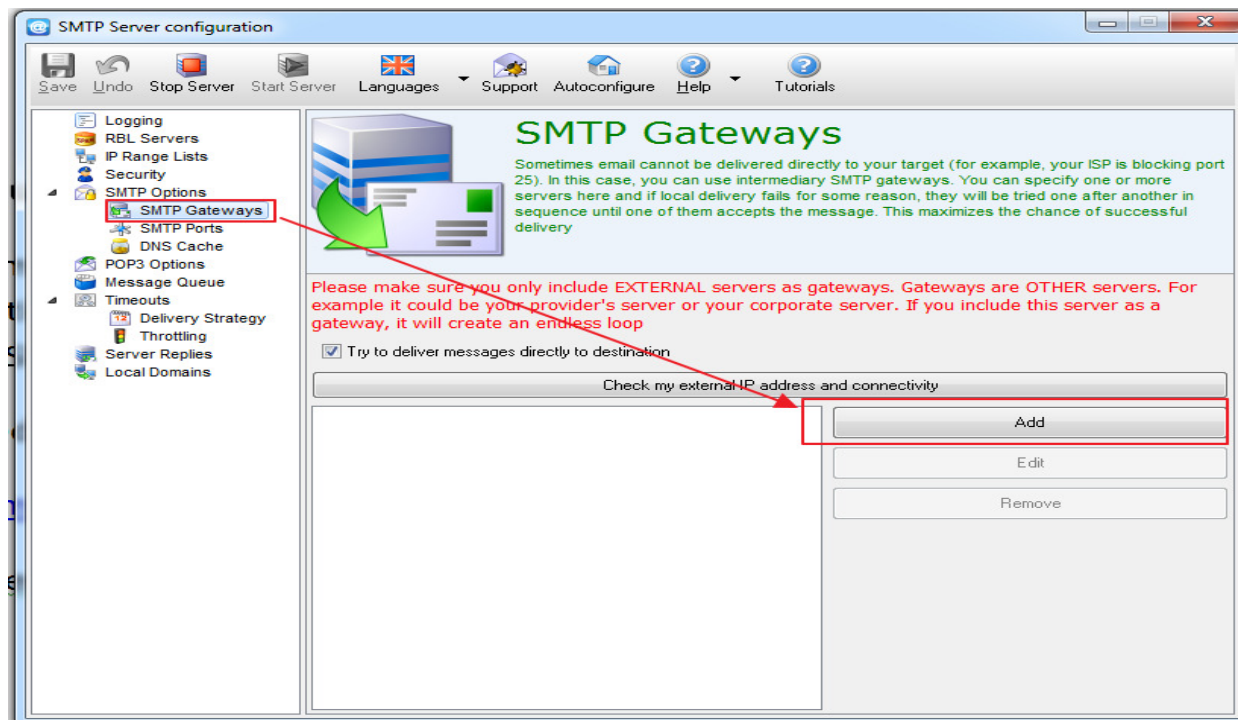
## Appendix C. To set up SMTP server, and enable [User Message] under ACTAtek3 device's Web UI

Step1. Please kindly check the company's IT department about the email server (SMTP setting). If it is required to setup the authentication while sending out the email. You can continue to step2 which will guide you to setup the localhost SMTP server to relay the emails to send out.

Step2. Please download Advanced SMTP Server at below link and install it.

<http://www.softstack.com/advsmtplib.html>

Step3. Run Advanced SMTP Server and click [Let me evaluate it] when the first time you run it. After that, please go to [SMTP Gateways] and click [Add] to configure your SMTP server with the correct authentication information required. See below as an example.



**Edit SMTP Gateway details**

**SMTP Host**  
SMTP Host usually looks like mail.domain.com or domain.com or smtp.domain.com. It can be IP address of your SMTP server that looks like four digits separated with dots, for example: 216.105.33.10

smtp.googlemail.com

**Authentication**  
User name : peter@actatek.com  
Password : ••••••••

Most of SMTP servers require authentication with user name and password. If your server requires authentication, enter your username and password in the boxes above.

**SMTP Port**  
Port 25 is standard SMTP port. Port 465 is standard for TLS. If your server uses TLS chances are it will respond to a different port. Check with your ISP

465

**Transport Layer Security (TLS)**  
☐ Do not use TLS  
☒ Implicit TLS. Protocol always starts with TLS  
☐ Require TLS. User commands are accepted only in TLS  
☐ Explicit TLS. Protocol will explicitly switch to TLS

Try the settings one by one if TLS is required and you are in doubt which one to use.

Please, give your email provider a call if you do not understand this screen. Ask them to help you configure your SMTP settings. Your email provider is probably your Internet Service Provider (ISP) if you use mail box provided by your ISP. It can be your web hosting provider if you use email account provided by your web hosting company.

Most of SMTP servers require authentication by user ID and password; many SMTP servers also require you to use Transport Level Security (TLS or SSL) or force you a port different from the standard. Among the standard TLS ports are port 465 and port 587.

If something does not work, we recommend you to play with the settings: try different TLS options and ports. Note that TLS usually works on a different port than the regular SMTP protocol.

Ok Cancel

After that, please click [Stop Server] and the [Start Server] to make the changes affect. Now you are ready to use the local PC's IP address as SMTP server to relay the emails to the external email address.

Step4.Login to ACTAtek device's Web UI->[Terminal Setup]->to setup the SMTP server's PC IP address where Advanced SMTP Server software was install.e.g.192.168.0.140 and the click [Submit].

**Terminal Settings**

- Holidays Setting
- Terminal Setup
- Authentication/Log Setup
- Terminal List
- Door Open Schedule
- Bell Schedule
- Connection Profile
- Terminal Clock
- External Devices

**Terminal**

- Cloud Storage Service
- SMS Service
- Alert Log
- Syslog
- Backup System Data
- Restore System Data

**Relay Delay** 8 sec (1-20)

☐ Disable  
☒ Door Strike 1 Clone  
☐ Access Denied  
☐ Bell Schedule  
☐ Active Alarm (Door Strike 2) When Door Opening Time Is Exceeded 30sec

**Relay Delay** 8 sec (1-20)  
 Note: Setting should not be changed while in operation

**IP Address:** Port: 80

**Manufacturer:** Axis **Model:** Axis 2100

**Language** English

**Webserver Port** 80 (80, 1024 - 65535)

**Allowed IP** ☒ Disable ☐ Enable (e.g. 192.168.1.\*)

**2-digit Duress Code**

**SMTP Server** 192.168.0.140

Submit Reset

Step5. Go to [User Message] to setup the user's email address. See below as an example. Also, you can configure the [Alter Log]. After that, every time when User ID:168 access the device, the device will send out email to inform the user or if there is any alert event log generated, the device will send out email to inform the administrator.

http://192.168.0.31/admin.html

**ACTAtek** The worldwide leader in Web based technologies.

**Terminal**

- Log Off
- Terminal Status

**User Administration**

- Attendance Report
- Daily Report
- View Event Log
- Add Event Log
- View User List
- Add New User
- Departments
- User Messages

**Access Control**

- Access Groups
- Triggers
- Holidays Setting

**Terminal Settings**

- Terminal Setup
- Authentication/Log Setup
- Terminal List
- Door Open Schedule
- Bell Schedule
- Connection Profile
- Terminal Clock
- External Devices

**Terminal**

- SMS Service
- Alert Log
- Syslog

## User Messages

[Add New Message Successful]

Add New Message  
[Accept 5 lines of texts: 25 Latin characters or 12 CJK characters per line with line-wrapping]

User ID: 168

User Message: TimeAttendance@Singapore Office

Character(s) Left: 100

☒ Show On LCD Screen ☒ Send to Email peter@actatek.com ☐ Notify to SMS

### Message List

<input type="checkbox"/>	No.	ID	Name	User Message	LCD	Email	SMS
<input type="checkbox"/>	1	168	Peter	TimeAttendance@Singapore Office	•	•	•

[Select All](#) | [Deselect All](#)

☐ Delete the message after display once

http://192.168.0.31/admin.html

**ACTAtek** The worldwide leader in Web based technologies.

**Terminal**

- Log Off
- Terminal Status

**User Administration**

- Attendance Report
- Daily Report
- View Event Log
- Add Event Log
- View User List
- Add New User
- Departments
- User Messages

**Access Control**

- Access Groups
- Triggers
- Holidays Setting

**Terminal Settings**

- Terminal Setup
- Authentication/Log Setup
- Terminal List
- Door Open Schedule
- Bell Schedule
- Connection Profile
- Terminal Clock
- External Devices

**Terminal**

- SMS Service
- Alert Log
- Syslog
- Backup System Data
- Restore System Data

## Alert Log Settings

Administrator's Email Address: peter@actatek.com


Administrator's SMS No:

NO.	Type	Email	SMS
1	Door is opened more than 30S	<input type="checkbox"/>	<input type="checkbox"/>
2	Bottom case is detached	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3	Primary is offline	<input type="checkbox"/>	<input type="checkbox"/>
4	Duress access	<input type="checkbox"/>	<input type="checkbox"/>

Step6.Login to your E-mail account to check the INBOX. See below as an example.

Note: If you did not receive the emails, please kindly check your [Spam] folder of the email account.

Search Images Mail Documents Calendar Sites Groups Contacts Mobile More »



peter@actatek.com ▾

Mail ▾

1-50 of 25,865

COMPOSE



Inbox (25,698)

Starred

Important

Sent Mail

Drafts (1)

You are invisible.  
[Go visible](#)

Spam Primavera - Toss with linguini, serve immediately Spam Recipe

<input type="checkbox"/>	☆	📧	me	Emergency Email From ACTAtek - 2012/09/27 17:32:42 Bottom Case is Detached! 00111DA0A767 ALERT!!!! It is an emergency email sent from	17:32
<input type="checkbox"/>	☆	📧	me	Emergency Email From ACTAtek - 2012/09/27 17:32:48 Bottom Case is Attached! 00111DA0A767 ALERT!!!! It is an emergency email sent from	17:32
<input type="checkbox"/>	☆	📧	me	Emergency Email From ACTAtek - 2012/09/27 17:32:41 Bottom Case is Attached! 00111DA0A767 ALERT!!!! It is an emergency email sent from	17:32
<input type="checkbox"/>	☆	📧	me	Emergency Email From ACTAtek - 2012/09/27 17:32:39 Bottom Case is Detached! 00111DA0A767 ALERT!!!! It is an emergency email sent from	17:32
<input type="checkbox"/>	☆	📧	me	ACTAtek Log - 168 2012/09/27 17:32:30 OUT User Message: TimeAttendance@Singapore Office	17:32
<input type="checkbox"/>	☆	📧	me	ACTAtek Log - 168 2012/09/27 17:32:21 IN User Message: TimeAttendance@Singapore Office	17:32

## Appendix D. Additional Security Options

### Auto IN/OUT:

- Admin users can enable this feature at 'Authentication /Log Setup' web page.

**ACTAtek** The worldwide leader in Web based technologies.

**Authentication/Log Setup**

**Log Setup**

Log Event ☐ Disable ☒ Enable

Log Size

Log Unauthorized Event ☒ Disable ☐ Enable

Accept Unregistered Smartcard ☒ Disable ☐ Enable

Photo Option for Log ☒ Authorized Event ☐ Unauthorized Event

**Authentication**

☐ Disable ☒ Auto IN/OUT ☐ Auto Reset IN/OUT

☐ Reject Repeated Event in  sec (1 - 86400)

☐ Anti-passback (Note: Anti-pass back will be reset at 00.00 hours)

☐ Lunch Break Lock Out  min (1 - 120)

- When this feature is enabled, the trigger set is 'Auto'.
- Triggers are automatically changed based on previous trigger status of individual user.



The picture above shows how Auto IN/OUT works.

- User login at 10.21 – his trigger is IN and event logs are updated
- User logout at 19.00 hours – his trigger type is automatically changed to OUT and event logs are updated.

Following screen shots shows the Time Attendance report and event logs:

Reports 1 of 1 << < 1 > >>

	User ID	Name	Date	Weekday	In Out	Total Working Hours
1	<a href="#">7588</a>	--	2012/03/16	Friday	10:21:06 19:00:12	8.65

Reports 1 of 1 << < 1 > >>

Event 1-2 of 2

&lt;&lt; &lt; 1 &gt; &gt;&gt;

	User ID	Name	Department	Date Time	Event	Terminal	Remark
1	7588	--	General	2012/03/16 19:00:12	OUT	ACTAtek	#SMC(SN:74DDF1EE)#
2	7588	--	General	2012/03/16 10:21:06	IN	ACTAtek	#SMC(SN:74DDF1EE)#

Event 1-2 of 2

&lt;&lt; &lt; 1 &gt; &gt;&gt;

Reset feature for Auto IN/OUT, if enabled, resets trigger at midnight (00.00 hrs)

**ACTAtek** The worldwide leader in Web based technologies.

**Authentication/Log Setup**

**Log Setup**

Log Event: ☐ Disable ☒ Enable

Log Size: 10 k

Log Unauthorized Event: ☒ Disable ☐ Enable

Accept Unregistered Smartcard: ☒ Disable ☐ Enable

Photo Option for Log: ☒ Authorized Event ☐ Unauthorized Event

**Authentication**

☐ Disable

☒ Auto IN/OUT ☐ Auto Reset IN/OUT

Additional Security Options:

☐ Reject Repeated Event in  sec (1 - 86400)

☐ Anti-passback (Note: Anti-pass back will be reset at 00.00 hours)

☐ Lunch Break Lock Out  min (1 - 120)

Submit Reset

Consider the following case:

### DAY 1

|-----|

Auto IN: 9.00

### DAY 2

|-----|

Auto IN - 9.00                      Auto OUT - 18.00

- On Day 1, user login, the trigger is Auto IN, event logs are updated.
- User forgets to logout (due to tailgating).
- As the Reset option for Auto IN/OUT is enabled, the triggers are reset over midnight
- Next day when the user login, the trigger is Auto IN, as per usual.
- Attendance for Day 1 is not calculated as there is no OUT trigger.

Following are the Time attendance and event logs screen shots

Reports 1-2 of 2							<< < 1 > >>	
	User ID	Name	Date	Weekday	In Out	Total Working Hours		
1	7588	--	2012/03/16	Friday	09:00:12 --	0.00		
2	7588	--	2012/03/17	Saturday	09:00:09 18:00:12	9.00		

Reports 1-2 of 2							<< < 1 > >>	
	User ID	Name	Department	Date Time	Event	Terminal	Remark	
1	7588	--	General	2012/03/17 18:00:12	OUT	ACTAtek	#SMC(SN:74DDF1EE)#	
2	7588	--	General	2012/03/17 09:00:09	IN	ACTAtek	#SMC(SN:74DDF1EE)#	
3	7588	--	General	2012/03/16 09:00:12	IN	ACTAtek	#SMC(SN:74DDF1EE)#	

### Reject Repeated Event:

- Admin user can enable this feature at 'Authentication/LogSetup' web page.

ACTAtek The worldwide leader in Web based technologies.

### Authentication/Log Setup

#### Log Setup

Log Event: ☐ Disable ☒ Enable

Log Size: 10 k

Log Unauthorized Event: ☒ Disable ☐ Enable

Accept Unregistered Smartcard: ☒ Disable ☐ Enable

Photo Option for Log: ☒ Authorized Event ☐ Unauthorized Event

#### Authentication

Additional Security Options:

☐ Disable

☐ Auto IN/OUT ☐ Auto Reset IN/OUT

☒ Reject Repeated Event in 10 sec(1 - 86400)

☐ Anti-passback (Note: Anti-pass back will be reset at 00.00 hours)

☐ Lunch Break Lock Out 0 min (1 - 120)

Submit Reset

- Reject repeat event duration in seconds has to be fill in, maximum duration being 86400 seconds. This duration is for the 'Reject repeat event' to be effective. When the duration is set to '0', 'Terminal setup failed – Invalid Limit for Reject repeated log' message would be displayed on web UI and the duration would be infinite.

- When this feature is enabled, the device detects repetition of any trigger type within the specified duration.
- Consider the following situation:



**Reject repeated login**

- User login using F1 trigger at 18.53.20
- He once again login using same trigger (F1) within 8 seconds. The device responds "Reject Repeated Login".
- But the subsequent login after the specified duration, will be successful and eventlogs are updated.

Following is the screenshot of event logs.

Event 1-4 of 4					<< < 1 > >>		
	User ID	Name	Department	Date Time ▼	Event	Terminal	Remark
1	7588	--	General	2012/03/15 18:53:48	F1	ACTAtek	#SMC(SN:74DDF1EE)#
2	7588	--	General	2012/03/15 18:53:42	IN	ACTAtek	#SMC(SN:74DDF1EE)#
3	7588	--	General	2012/03/15 18:53:27	REJECTED	ACTAtek	#SMC(SN:74DDF1EE)#
4	7588	--	General	2012/03/15 18:53:20	F1	ACTAtek	#SMC(SN:74DDF1EE)#
Event 1-4 of 4					<< < 1 > >>		

**Anti-pass back:**

The main purpose of anti-pass back system is to prevent a card holder from passing their card back to a second person to gain entry into the same controlled area. This also improves the accuracy of roll call 'Last Known position' reports and deters tailgating. Anti-pass back sequence being 'IN-OUT-IN-OUT-IN-OUT'. If the user logs IN using his card and then passes his card back to a friend, the card would not work the second time. Because the attempt to use card second time would create IN-IN sequence that is violation of anti-pass back rules. Admin users can enable this feature at 'Authentication/Log Setup' web page.

ACTAtek The worldwide leader in Web based technologies.

**Terminal**

- Log Off
- Terminal Status

**User Administration**

- Attendance Report
- Daily Report
- View Event Log
- Add Event Log
- View User List
- Add New User
- Departments
- User Messages

**Access Control**

- Access Groups
- Triggers
- Job Code
- Holidays Setting

**Terminal Settings**

- Terminal Setup
- Authentication/Log Setup
- Terminal List
- Door Open Schedule
- Bell Schedule
- Connection Profile
- Terminal Clock
- External Devices

**Authentication/Log Setup**

**Log Setup**

Log Event: ☐ Disable ☒ Enable

Log Size: 10 k

Log Unauthorized Event: ☒ Disable ☐ Enable

Accept Unregistered Smartcard: ☒ Disable ☐ Enable

Photo Option for Log: ☒ Authorized Event ☐ Unauthorized Event

**Authentication**

☐ Disable

☐ Auto IN/OUT ☐ Auto Reset IN/OUT

☐ Reject Repeated Event in  sec(1 - 86400)

☒ Anti-passback (Note: Anti-pass back will be reset at 00.00 hours)

☐ Lunch Break Lock Out  min (1 - 120)

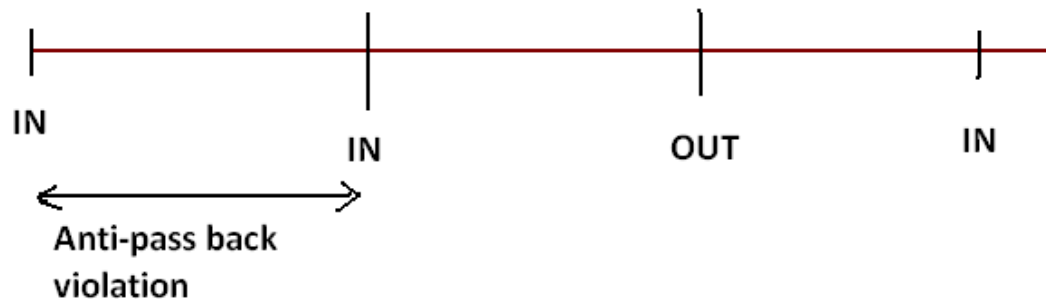
Submit Reset

Consider the following case:



- This is the normal anti-pass back sequence.
- As long as the user follows 'IN-OUT-IN-OUT' sequence, there will be no violations.

Consider the following case:



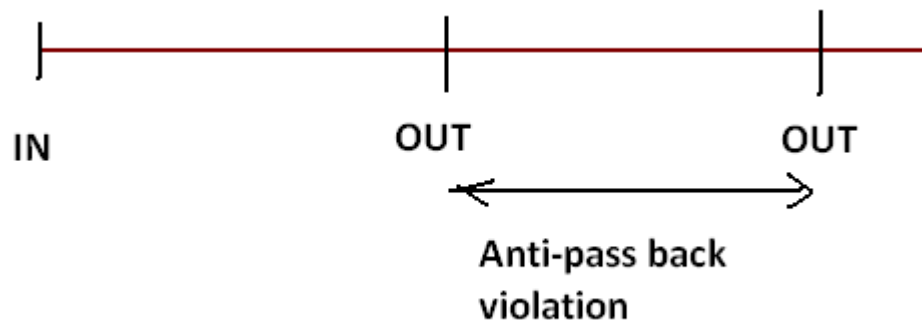
- User login (FP/Smart card/password user), upon successful authentication, event logs are updated.
- User login once again, the sequence 'IN-IN' is generated which is anti-pass back violation. And hence an error message "Anti-pass back violation" would be displayed without granting access to the second user and event log (rejected event) will be updated.

Following is the screen shot of event logs being generated:

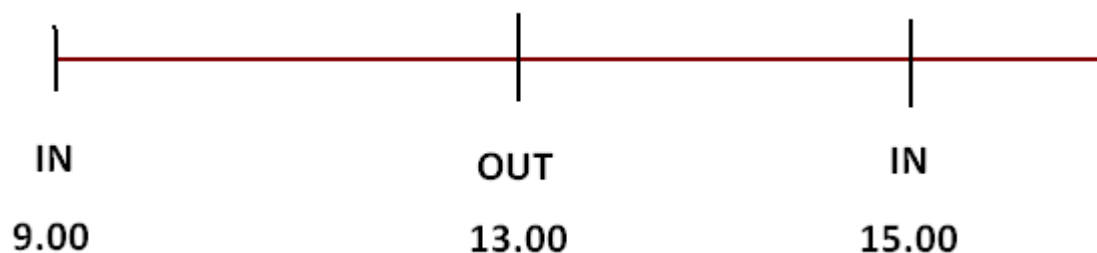
Event 1-4 of 4							<< < 1 > >>
	User ID	Name	Department	Date Time	Event	Terminal	Remark
1	7588	--	General	2012/03/15 18:33:28	IN	ACTAtek	#SMC(SN:74DDF1EE)#
2	7588	--	General	2012/03/15 18:33:23	OUT	ACTAtek	#SMC(SN:74DDF1EE)#
3	7588	--	General	2012/03/15 18:33:06	REJECTED	ACTAtek	#SMC(SN:74DDF1EE)#
4	7588	--	General	2012/03/15 18:33:01	IN	ACTAtek	#SMC(SN:74DDF1EE)#

Event 1-4 of 4 << < 1 > >>

Following is another example of anti-pass back violation:



Anti-pass back is reset at midnight 00.00 hours.  
Consider the following condition:



- User login using IN trigger, upon successful authentication event logs are updated.
- User logout using OUT trigger, event log is updated.
- User login once again 'IN-OUT-IN', user is granted access and event log is updated.
- But the user forgets to logout due to tailgating.
- Next day when the user login, he is granted IN access as per usual, as the triggers are reset in midnight (00.00 hours).

Following is the screen shot of event logs being generated:

Event 1-4 of 4							<< < 1 > >>
	User ID	Name	Department	Date Time	Event	Terminal	Remark
1	7588	--	General	2012/03/16 09:00:08	IN	ACTAtek	#SMC(SN:74DDF1EE)#
2	7588	--	General	2012/03/15 15:00:11	IN	ACTAtek	#SMC(SN:74DDF1EE)#
3	7588	--	General	2012/03/15 13:00:13	OUT	ACTAtek	#SMC(SN:74DDF1EE)#
4	7588	--	General	2012/03/15 09:01:01	IN	ACTAtek	#SMC(SN:74DDF1EE)#
Event 1-4 of 4							<< < 1 > >>

### Lunch Break / Lock Out:

Admin user can enable this feature @ 'Authentication/Log Setup' web page.  
Lunch duration called 'lock out' can be fixed between the range 1 to 120 minutes. Default value being 30 minutes.

The screenshot shows the 'Authentication/Log Setup' web page. The sidebar on the left contains the following navigation links:

- Terminal**
  - Log Off
  - Terminal Status
- User Administration**
  - Attendance Report
  - Daily Report
  - View Event Log
  - Add Event Log
  - View User List
  - Add New User
  - Departments
  - User Messages
- Access Control**
  - Access Groups
  - Triggers
  - Job Code
  - Holidays Setting
- Terminal Settings**
  - Terminal Setup
  - Authentication/Log Setup
  - Terminal List
  - Door Open Schedule
  - Bell Schedule
  - Connection Profile
  - Terminal Clock
  - External Devices

The main content area is titled 'Authentication/Log Setup' and contains two sections:

#### Log Setup

- Log Event: ☐ Disable ☒ Enable
- Log Size: 10 k
- Log Unauthorized Event: ☒ Disable ☐ Enable
- Accept Unregistered Smartcard: ☒ Disable ☐ Enable
- Photo Option for Log: ☒ Authorized Event ☐ Unauthorized Event

#### Authentication

- ☐ Disable
- ☐ Auto IN/OUT ☐ Auto Reset IN/OUT
- ☐ Reject Repeated Event in  sec (1 - 86400)
- ☐ Anti-passback (Note: Anti-pass back will be reset at 00.00 hours)
- ☒ Lunch Break Lock Out  min (1 - 120)

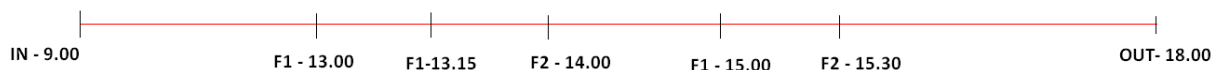
At the bottom of the Authentication section are 'Submit' and 'Reset' buttons.

All the triggers are available to the user when this feature is enabled.

Following are the triggers used to implement the logic:

1. IN – This trigger is considered for user login, IN time is recorded for generating attendance report.
2. OUT – This is considered as user logout and OUT time is recorded for generating attendance report.
3. F1 – Lunch IN trigger. Only the first lunch IN time will be recorded. This time can be viewed and Reset @ 'View User List/Modify User'. The first lunch IN time is used to calculate the lock out duration for individual user. First lunch IN time will be reset for all the users, every midnight at 00.00 hours.
4. F2 – Lunch OUT trigger. User is allowed to use F2, only when he has first lunch IN time and has over lock out duration. Upon successful lunch OUT, the first lunch IN time will be reset, thus allowing user to have second lunch in.

Consider the following case:



- User login at 9.00 hours and logout at 18.00 hours
- First lunch in is at 13.00 hours.
- The subsequent F1 triggers will not be considered for calculation of lock out period. But event logs will be updated.

Following is the screen shot of attendance report and event logs being generated:

Reports 1 of 1										<< < 1 > >>	
	User ID	Name	Date	Weekday	In Out	In Out	LunchIn LunchOut	LunchIn LunchOut	Total Working Hours		
1	1981	--	2012/03/15	Thursday	09:00:13 18:00:50	18:00:43 --	13:00:13 14:00:15	15:00:13 15:30:14	7.51		
Reports 1 of 1										<< < 1 > >>	

**Working Hours** (18.00 - 9.00 ) = 9 hours  
**Lunch 1** (14.00 - 13.00) = 1 hour  
**Lunch 2** (15.30 - 15.00) = 0.5 hour

**Total working hours** (working hour - (lunch 1 + lunch 2))  
 (9 - (1 + 0.5)) = 7.5

Event 1-9 of 9

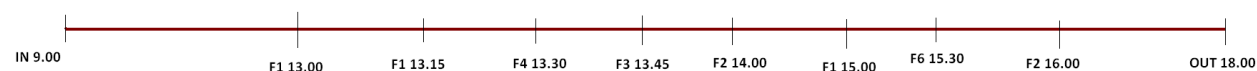
&lt;&lt; &lt; 1 &gt; &gt;&gt;

	User ID	Name	Department	Date Time	Event	Terminal	Remark
1	<a href="#">1981</a>	--	General	2012/03/15 18:00:50	OUT	ACTAtek	#FP#
2	<a href="#">1981</a>	--	General	2012/03/15 18:00:43	IN	ACTAtek	#FP#
3	Unknown User	--	--	2012/03/15 18:00:36	REJECTED	ACTAtek	#FP(ID:)#
4	<a href="#">1981</a>	--	General	2012/03/15 15:30:14	F2	ACTAtek	#FP#
5	<a href="#">1981</a>	--	General	2012/03/15 15:00:13	F1	ACTAtek	#FP#
6	<a href="#">1981</a>	--	General	2012/03/15 14:00:15	F2	ACTAtek	#FP#
7	<a href="#">1981</a>	--	General	2012/03/15 13:15:16	F1	ACTAtek	#FP#
8	<a href="#">1981</a>	--	General	2012/03/15 13:00:13	F1	ACTAtek	#FP#
9	<a href="#">1981</a>	--	General	2012/03/15 09:00:13	IN	ACTAtek	#FP#

Event 1-9 of 9

&lt;&lt; &lt; 1 &gt; &gt;&gt;

Consider another example:



- User has used several triggers throughout the day.
- Logic to generate Attendance report still remains the same.

Following are the screen shots of attendance report and event logs:

Reports 1 of 1

&lt;&lt; &lt; 1 &gt; &gt;&gt;

	User ID	Name	Date	Weekday	In Out	In Out	LunchIn LunchOut	LunchIn LunchOut	Total Working Hours
1	<a href="#">7588</a>	--	2012/03/15	Thursday	09:00:12 18:00:13	14:00:18 --	13:00:15 14:00:26	15:00:18 16:00:14	7.00

Reports 1 of 1

&lt;&lt; &lt; 1 &gt; &gt;&gt;

Working hours (18.00 - 9.00) = 9 hours

Lunch 1 (F2 - F1)

(14.00 - 13.00) = 1 hour

Lunch 2 (16.00 - 15.00) = 1 hour

Total Working hour (Working hour - (Lunch 1 + Lunch 2))

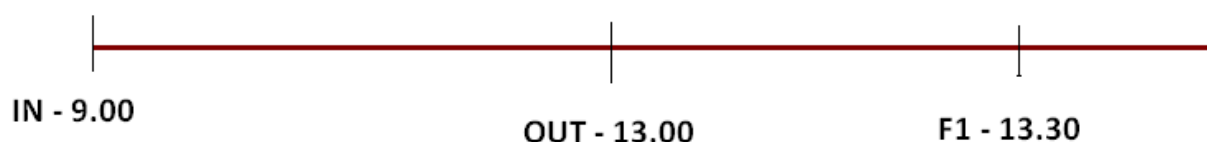
(9 - (1 + 1)) = 7 hours

Event 1-11 of 11 << < 1 > >>

	User ID	Name	Department	Date Time	Event	Terminal	Remark
1	7588	--	General	2012/03/15 18:00:13	OUT	ACTAtek	#SMC(SN:74DDF1EE)#
2	7588	--	General	2012/03/15 16:00:14	F2	ACTAtek	#SMC(SN:74DDF1EE)#
3	7588	--	General	2012/03/15 15:30:16	F6	ACTAtek	#SMC(SN:74DDF1EE)#
4	7588	--	General	2012/03/15 15:00:18	F1	ACTAtek	#SMC(SN:74DDF1EE)#
5	7588	--	General	2012/03/15 14:00:26	F2	ACTAtek	#SMC(SN:74DDF1EE)#
6	7588	--	General	2012/03/15 14:00:18	IN	ACTAtek	#SMC(SN:74DDF1EE)#
7	7588	--	General	2012/03/15 13:45:14	F3	ACTAtek	#SMC(SN:74DDF1EE)#
8	7588	--	General	2012/03/15 13:30:11	F4	ACTAtek	#SMC(SN:74DDF1EE)#
9	7588	--	General	2012/03/15 13:15:11	F1	ACTAtek	#SMC(SN:74DDF1EE)#
10	7588	--	General	2012/03/15 13:00:15	F1	ACTAtek	#SMC(SN:74DDF1EE)#
11	7588	--	General	2012/03/15 09:00:12	IN	ACTAtek	#SMC(SN:74DDF1EE)#

Event 1-11 of 11 << < 1 > >>

Consider another example:



Always the lunch IN/OUT time lies within user log IN/OUT range.

If the Lunch IN (F1) trigger happens after OUT trigger, then it is considered as invalid entry.

**Error message: Invalid Entry**

**Working Hours:** (13.00 - 9.00) = 4 hours

**Total working hours:** 4 hours

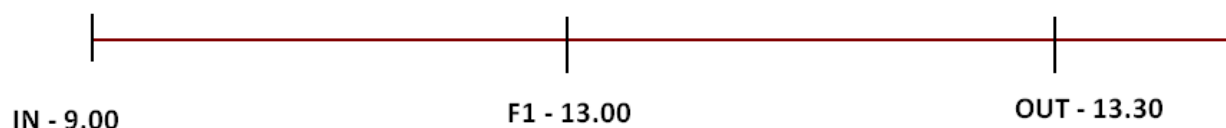
Reports 1 of 1 << < 1 > >>

	User ID	Name	Date	Weekday	In Out	Total Working Hours
1	7588	--	2012/03/15	Thursday	09:00:12 13:00:11	4.00

Reports 1 of 1 << < 1 > >>

First lunch IN time for all the users will be reset at midnight (00.00 hours).

Consider the following case:



- User is having a valid IN and OUT event.
- But after lunch IN, the user forgets to do lunch out due to tailgating.

- User logs IN the next day. For lunch out authentication, the first lunch in made by the user after 00.00 hours will be considered for calculation and not the lunch IN time that he made the previous day.

Following is the attendance and event log screen shots:

Reports 1 of 1							<< < 1 > >>
	User ID	Name	Date	Weekday	In Out	LunchIn LunchOut	Total Working Hours
1	<a href="#">7588</a>	--	2012/03/15	Thursday	09:00:11 13:30:10	13:00:14 --	4.50

Reports 1 of 1							<< < 1 > >>
----------------	--	--	--	--	--	--	-------------

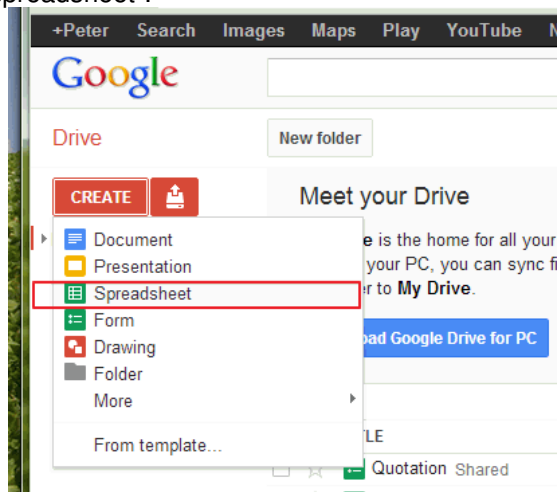
Event 1-3 of 3							<< < 1 > >>
	User ID	Name	Department	Date Time ▼	Event	Terminal	Remark
1	<a href="#">7588</a>	--	General	2012/03/15 13:30:10	OUT	ACTAtek	#SMC(SN:74DDF1EE)#
2	<a href="#">7588</a>	--	General	2012/03/15 13:00:14	F1	ACTAtek	#SMC(SN:74DDF1EE)#
3	<a href="#">7588</a>	--	General	2012/03/15 09:00:11	IN	ACTAtek	#SMC(SN:74DDF1EE)#

Event 1-3 of 3							<< < 1 > >>
----------------	--	--	--	--	--	--	-------------

## Appendix E. Cloud Storage Service

Step1. Login to your personal or company's Google Drive account.  
<https://drive.google.com/>

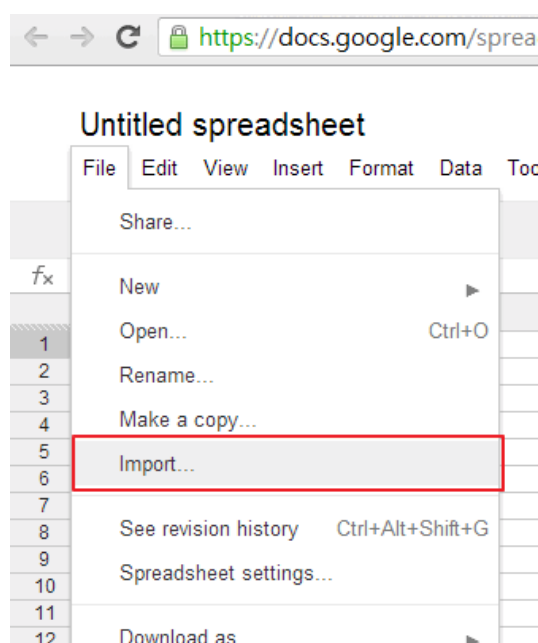
Step2. Create a "new spreadsheet".



Step3. Download and import the "template event log file", and then "open" a new spreadsheet. See below.

Note: Download link of "template eventlog file"

<http://www.actatek.com/Downloads/actatek3/support/template%20eventlog.csv>



<https://docs.google.com/spreadsheet/ccc?key=0AsbYlt7QhIvXdEhfYWJXS1hRek5QTTh1WGtCSmFwNmc#gid=C>

Import file

**Upload file**  
Supported formats: .xls, .xlsx, .ods, .csv, .txt, .tsv, .tab

[Open file](#) template eventlog.csv

**Import action**

☒ Create new spreadsheet

☐ Insert new sheet(s)

☐ Replace spreadsheet

☐ Replace current sheet

☐ Append rows to current sheet

☐ Replace data starting at selected cell

**Separator character**

☒ Automatic

☐ Tab

☐ Comma

☐ Custom:

[Import](#) [Cancel](#)

**Preview**

	A	B	C	D	E
1	rid	userid	terminals	eventid	event
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					

<https://docs.google.com/spreadsheet/ccc?key=0AsbYlt7QhIvXdEhfYWJXS1hRek5QTTh1WGtCSmFwNmc#gid=C>

Import file

**Upload file**  
Supported formats: .xls, .xlsx, .ods, .csv, .txt, .tsv, .tab

[Open file](#) template eventlog.csv

File imported successfully. [Open now »](#)

**Import action**

☒ Create new spreadsheet

☐ Insert new sheet(s)

☐ Replace spreadsheet

☐ Replace current sheet

☐ Append rows to current sheet

☐ Replace data starting at selected cell

**Separator character**

☒ Automatic

☐ Tab

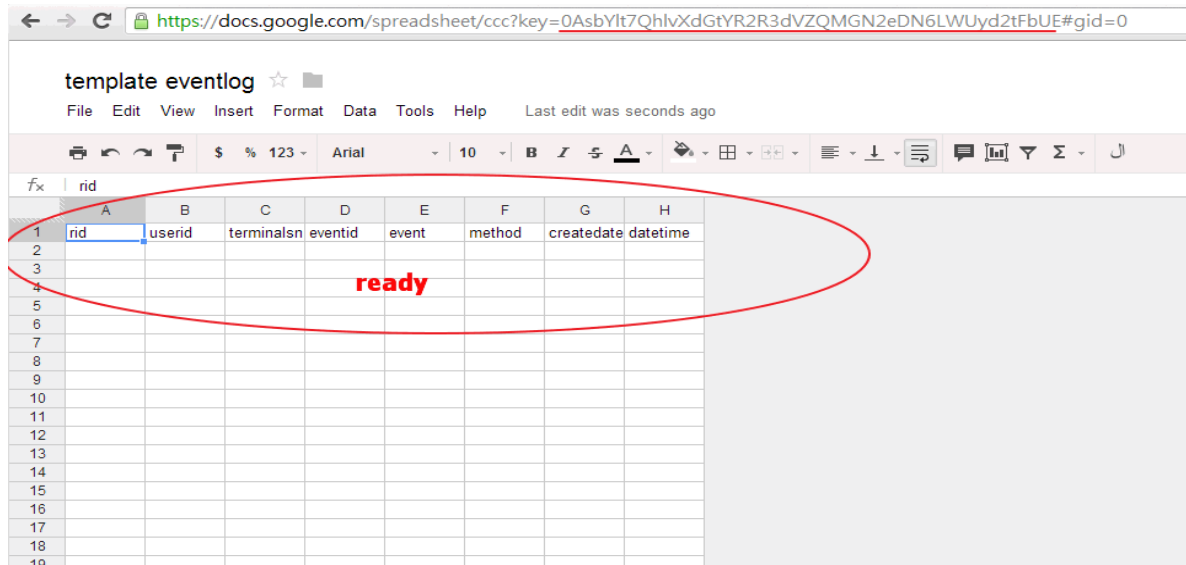
☐ Comma

☐ Custom:

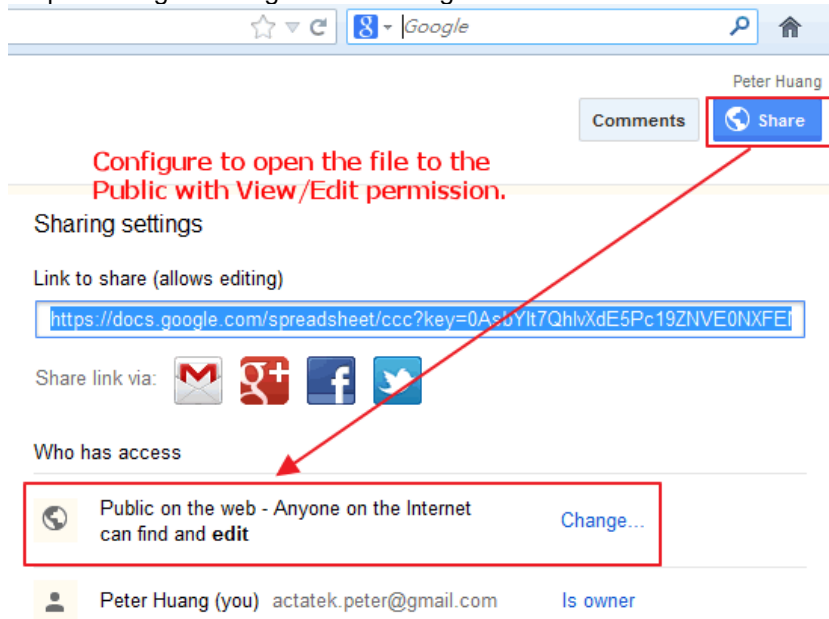
[Import](#) [Cancel](#)

**Preview**

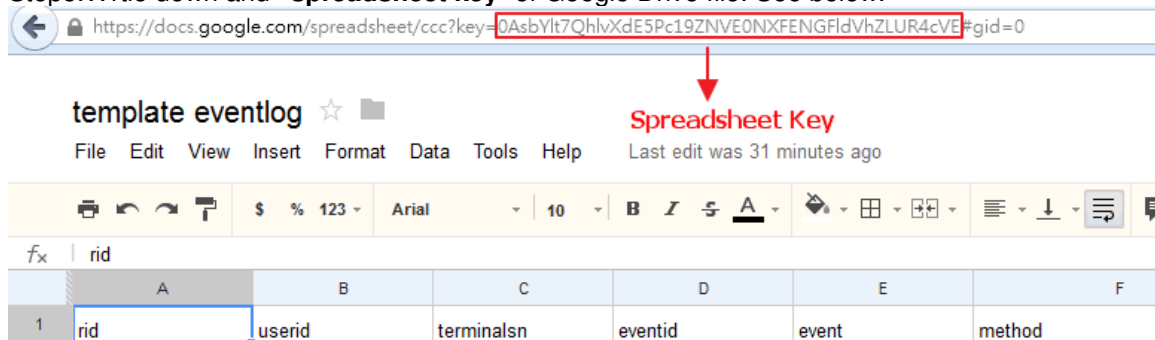
	A	B	C	D	E
1	rid	userid	terminals	eventid	event
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					



Step4. Configure Google Drive setting about who can access the file. See below.



Step5. Write down and “spreadsheet key” of Google Drive file. See below.



Step6.Login to ACTAtek3's Web UI to set up ,and enable ACTAtek3's Cloud Storage Service with correct login detail and right new created Google Doc spreadsheet key. See below.

**ACTAtek** The worldwide leader in Web based technologies.

### Cloud Storage Service

#### Login Setup

Cloud Storage Service: Google Drive

Email: sivaiah.patel@gmail.com

Password: .....

Spreadsheet Key: 0AsbYlt7QhlyXdE5Pc19ZNVE0NXFENGfIdVhZLUR4cVE

Worksheet ID: od6 → **od6**

#### Upload Data Field

Enable	Field Name
<input checked="" type="checkbox"/>	UserID
<input checked="" type="checkbox"/>	Timestamp
<input checked="" type="checkbox"/>	Local Timestamp
<input checked="" type="checkbox"/>	EventID
<input checked="" type="checkbox"/>	Remark
<input checked="" type="checkbox"/>	TerminalSN

Submit Reset

**Your Google Drive Login detail & the file's spreadsheet key.**

Step7.After that, please do the "hardware reboot".(power off & power on).

Step8.After the device reboot, the user can start to access the device to generate new event logs which the new event logs will be pushing to Google drive file. You can open your Google Doc link to check the event logs any time from any place. See below.

actatek3\_google\_cloud\_integration

	rid	useric	terminalsn	eventid	event	method	createdate	datetime
233	4	147	00111DA05037	1	IN	FP	4/12/2013 8:31:46	4/12/2013 8:31:46
234	4	147	00111DA05037	1	IN	FP	4/12/2013 8:31:51	4/12/2013 8:31:51
235	4	147	00111DA05037	1	IN	FP	4/12/2013 8:31:55	4/12/2013 8:31:55
236	4	147	00111DA05037	1	IN	FP	4/12/2013 8:32:00	4/12/2013 8:32:00
237	4	147	00111DA05037	1	IN	FP	4/12/2013 8:32:06	4/12/2013 8:32:06
238	4	147	00111DA05037	1	IN	FP	4/12/2013 8:32:11	4/12/2013 8:32:11
239	4	147	00111DA05037	1	IN	FP	4/12/2013 8:32:15	4/12/2013 8:32:15
240	3	123	00111DA05037	1	IN	FP	4/12/2013 8:32:20	4/12/2013 8:32:20
241	3	123	00111DA05037	1	IN	FP	4/12/2013 8:32:26	4/12/2013 8:32:26
242	3	123	00111DA05037	1	IN	FP	4/12/2013 8:32:31	4/12/2013 8:32:31
243	3	123	00111DA05037	1	IN	FP	4/12/2013 9:04:35	4/12/2013 9:04:35
244	2	168	00111DA05037	1	IN	FP	4/12/2013 9:04:40	4/12/2013 9:04:40
245	2	168	00111DA05037	1	IN	FP	4/12/2013 9:04:45	4/12/2013 9:04:45
246	2	168	00111DA05037	2	OUT	FP	4/12/2013 9:05:01	4/12/2013 9:05:01
247	2	168	00111DA05037	1	IN	FP	4/12/2013 9:05:08	4/12/2013 9:05:08
248	2	168	00111DA05037	2	OUT	FP	4/12/2013 9:05:14	4/12/2013 9:05:14
249	2	168	00111DA05037	1	IN	FP	4/12/2013 9:06:13	4/12/2013 9:06:13
250	2	168	00111DA05037	1	IN	FP	4/12/2013 17:06:24	4/12/2013 17:06:24

## Appendix F. Short Message Service(SMS)

Step1.Login to ACTAtek Web Admin Page and then go to [Terminal]->[SMS Service] .See below.

The screenshot shows the ACTAtek Web Admin interface. The left sidebar contains a menu with categories: Departments, User Messages, Access Control, Terminal Settings, and Terminal. The 'Access Control' category is expanded, showing sub-items like Access Groups, Triggers, Job Code, and Holidays Setting. The 'Terminal Settings' category is also expanded, showing sub-items like Terminal Setup, Authentication/Log Setup, Terminal List, Door Open Schedule, Bell Schedule, Connection Profile, Terminal Clock, and External Devices. The 'Terminal' category is expanded, showing sub-items like Cloud Storage Service, SMS Service, Alert Log, and Syslog. The main content area is titled 'Short Message Service(SMS)' and contains a form with the following fields: SMS Service (dropdown menu set to SMS.sg), SMS User ID (text box containing actatek.support), and SMS Password (password box with four dots). There are Submit and Reset buttons at the bottom of the form.

Note1: Make sure that ACTAtek3's IP settings are correct, and can access the Internet

Note2: The "SMS User ID" and the "SMS Password" can get from <http://SMS.SG> who provided the SMS Gateway Services. More information can be found at their website at <http://SMS.SG>

Step2.Go to [User Messages] to set up the User Message and select [Notify to SMS] . See below.

The screenshot shows the ACTAtek Web Admin interface. The left sidebar is the same as in the previous screenshot. The main content area is titled 'User Messages' and contains a message '[Add New Message Successful]'. Below this is a section 'Add New Message' with a note '[Accept 5 lines of texts: 25 Latin characters or 12 CJK characters per line with line-wrapping]'. The form has the following fields: User ID (text box containing 168), User Message (text area containing Time Attendance), and Character(s) Left (text box containing 125). There are checkboxes for 'Show On LCD Screen' (checked), 'Send to Email' (unchecked), and 'Notify to SMS' (checked). The 'Notify to SMS' checkbox is linked to a text box containing +6585562789. There are Submit and Reset buttons. Below the form is a 'Message List' section with a table. The table has columns: No., ID, Name, User Message, LCD, Email, and SMS. The first row shows a message with ID 168, Name David Wong, and User Message Time Attendance. There are links for 'Select All' and 'Deselect All' below the table. There is a 'Delete' button and a checkbox 'Delete the message after display once' with a 'Confirm' button.

No.	ID	Name	User Message	LCD	Email	SMS
1	168	David Wong	Time Attendance	•	•	•

Step3(Optional): You can also set up on sending the Alert Log via SMS or email and then click [Submit] . See below.

The screenshot shows a web browser window with the URL <http://192.168.1.100/admin.htr>. The page title is "ACTAtek The worldwide leader in Web based technologies." The left sidebar contains a menu with the following items:

- Daily Report
- View Event Log
- Add Event Log
- View User List
- Add New User
- Departments
- User Messages
- Access Control**
  - Access Groups
  - Triggers
  - Job Code
  - Holidays Setting
- Terminal Settings**
  - Terminal Setup
  - Authentication/Log Setup
  - Terminal List
  - Door Open Schedule
  - Bell Schedule
  - Connection Profile
  - Terminal Clock
  - External Devices
- Terminal**
  - Cloud Storage Service
  - SMS Service
  - Alert Log

The main content area is titled "Alert Log Settings". It contains two input fields:

- Administrator's Email Address:
- Administrator's SMS No:

Below these fields is a table with the following data:

NO.	Type	Email	SMS
1	Door is opened more than 30S	<input type="checkbox"/>	<input type="checkbox"/>
2	Bottom case is detached	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
3	Primary is offline	<input type="checkbox"/>	<input type="checkbox"/>
4	Duress access	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

At the bottom left of the table area is a "Submit" button. At the bottom right is the text "Copyright © 2001".

Example. User ID: 111 access the ACTAtek Unit as "IN event". The ACTAtek will send the SMS via <http://SMS.SG> services provider to the mobile phone number directly. See below.



worldwide leader in Web based technologies

### Event Log

Search Options:

Name  ID

User

Period  or From  To

Time Today  or 2011/5/6  2011/5/6

Department  Event

Others

Fill in the form to filter the report, or leave it blank for a full report

Event 1-3 of 3

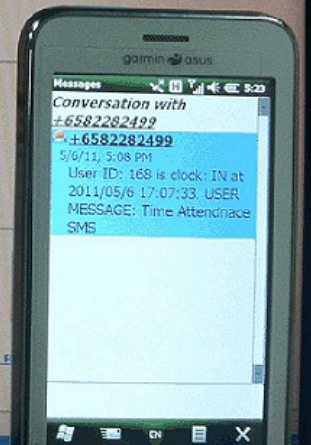
#	User ID	Name	Department	Date Time	Event	Terminal	Captured Image	Remark
1	168	Peter Huang	General	2011/05/06 17:07:33	IN	ACTAtek	<a href="#">View Image</a>	#FP#
2	168	Peter Huang	General	2011/05/06 17:02:38	OUT	ACTAtek	<a href="#">View Image</a>	#FP#
3	168	Peter Huang	General	2011/05/06 17:02:03	IN	ACTAtek	<a href="#">View Image</a>	#FP#

Event 1-3 of 3

Delete Event Log

Delete all event logs before the beginning of:

Copyright © 2001-2009 by ACTAtek Pte. Ltd.



## Appendix G. FingerPrint enrollment notes

### Step One

### Choosing The "Best" Fingerprint

Use either your Index, Middle or Ring finger, when enrolling and verifying your fingerprint. Avoid using the Pinky finger, as it is typically difficult to align it properly and consistently. Choose a finger that can produce the best fingerprint.

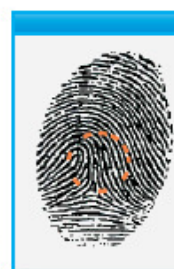


The ACTAtek does not store a picture of your fingerprint.

### 2

### Locating The Fingerprint "Core"

The "core" of a fingerprint is defined as the point located within the inner most recurving ridge. It is extremely important that this area is identified, and placed on the center of the fingerprint scanner during the enrollment and verification of your fingerprint.



### 3

### Prepare The Finger for Enrollment

When enrolling and verifying with your fingerprint it is important that your finger be clean. It is also recommended that the finger be relatively undamaged and without scars.



Washing your hands with moisturizing soap and using hand lotion will also improve accuracy!

### Step 4: Finger Placement

When placing your finger on the scanner, make sure that the location of the "core", located in Step 2, is making direct contact with the scanner. Apply medium pressure, or just enough to flatten the skin on your finger.

