ACTA4 User Manual

Version 2.1

February , 2026

Jakin ID

ACTA4 User Manual

Offices:

Asia and the Rest of the World:

Unit 913-914, 9/F., Worldwide Industrial Centre, 43-47 Shan Mei Street

Fotan, Shatin, N.T., Hong Kong

Tel: (+852) 2319 1333

Email: info@jakinid.com

Americas (North and South America):

411-1221 HOMER ST,VANCOUVER BC V6B 1C5
Canada

Phone: (+1) 604 314 7628
Email: info@jakinid.com

Europe, Middle East & Africa:

86-90 Paul St, London EC2A 4NE, U.K..

Phone: (+44) 7344 2638 81
Email: info@jakinid.com

Table of Contents

Chapter 1. Introduction

This section explains the purpose and software references of the ACTA4.

1.1. Purpose

ACTA4 devices are the IoT hardware platform of a cloud- and web-based ID management solution for security and Human Resource Management. The ACTA4 device allows users to access its record from anywhere, at any time and on any ICT platform using any web-browsers such as Edge, Firefox, Chrome, Safari etc.

This document aims to help you use the basic and advanced features of ACTA4 effectively. This document also aims to help you troubleshoot the ACTA4 quickly if you encounter any issues during installation and usage. By reading this user manual, you will learn more about the functions and features of ACTA4.

Some of the features and functions require working with the ACTAtek Access Manager Suite (AMS) software. The Emergency Exit function is designed to be used for the traditional 3rd party controller panel system.

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 ACTA4. Advanced customers can use this document to enhance their usage in ACTA4, and resellers can use this document to enhance their customers' needs.

1.4. Software References for this document

ACTA4 firmware: 4_00.2540 or above version

Chapter 2. Product Overview

2.1. Physical Security:

Access control

Our Biometrics, RFID IoTs fit well with all entrances: doors, gates, turnstiles, carpark barriers etc, regardless it's for the security deposit box, access control, video surveillance or integration with all of them. It can be installed to suit all businesses:

1. **Stand-alone installation**: Plug the IoT to your network, connecting to the electric door strike which can also be powered by the device if needed. Simply use any web-browser just like internet banking to manage users, browse reports and device administration etc

2. **Master/Client setup**: You can connect up to 10 units within your network without any computers! All user attributes and event logs are synchronized to the Master and other Client units.

3. **Enterprise scale installation**: All units can be pointed to the AMS or AMS SaaS cloud application platform with both applications for access control and workforce management applications. The AMS or AMS SaaS takes care of everything!

2.2. Workforce Management:

Time Attendant

For standalone units, there are time attendance reports available including total working hours.

The AMS or AMS SaaS cloud platform with both workforce management and access control applications can generate many time attendance reports, shift management, job-codes etc to suit the need of large enterprises.

Payroll

Our IoTs can output event logs directly to CSV/TXT file for the 3rd party's payroll APP integration.

The AMS SOAP/API allows the 3rd party system integration from different databases support such as Oracle, SQL, MySQL Azure SQL/MySQL etc.

2.3. Benefits:

1. All-in-one IP-video, Intercom and door bell biometrics, RFID, IoT securing access to all the entrances, throw away the keys and making a huge saving in managing and issuing the keys!

2. Access control of all entrances with individual or group access rights in terms of time and door access!

3. All-in-one video surveillance, access control and time clock for main and all doors!

4. Support legacy RFID cards, no need to reissue the cards!

5. Offers POE and power to the strikes using just the Cat5/6 cable, saving all the costs of cables and cabling!

6. Wiegand out allows integration back to any traditional control panel.

7. Online maintenance saving expensive manpower and on-site visits!

8. Double up as a time clock for workforce management for free!

Our SOAP based API/SDK allows integration to Oracle, SQL, SAP, Azure SQL etc, please check below link:

http://www.jakinid.com/supportkb/knowledgebase.php?category=24

2.4. Introduction Videos

Unlike Traditional access control products, our devices are IoTs connecting directly to the internet and can work online and off-line so that no one gets stuck behind the door:

Meanwhile, please view our ACTA IoT device and the private cloud software AMS video in the below links:

Jakin ID Unified Edge IoT Solution: Smart Security & Energy Management

https://www.youtube.com/watch?v=jYpp7yAKFc4

Enhancing Safety & EHS with Jakin IoT Solutions

https://www.youtube.com/watch?v=bB0Rz_oiygE

2.5. IP Intercom

The IoT can also has IP intercom as an option talking to SIP client software or apps on your PC or mobile phone. (Please refer to **Appendix J** for more information.)

2.6. Car parks, turnstiles, gates and perimeter control

The IoTs can be used to control all the vehicles entry to car parks, turnstiles, gates, and perimeters

2.7. Visitor Management

All visitors can be issued with temporary credential with pre-determined hours or access and other access rights by RFID cards, biometrics or PIN.

2.8. ACTA4 Model number

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

Table 1.ACTA4 Model Number

2.8.1. Legend

Model	*Meaning*
10k (smartcard, camera, fingerprint)	Embedded SSL-Web Server up to 10,000 users
20k	Embedded SSL-Web Server up to 20,000 users
50k (max. users of fingerprint only)	Embedded SSL-Web Server up to 50,000 users
100k (max. users of smartcard only)	Embedded SSL-Web Server up to 100,000 users
Option	***Meaning***
P	Pin Model
C	Built-in Video /Camera Model /Facial model
S (M / E / Hp / Hi / STa/ EXBC)	Smart Card Model (**M**: MiFare 4bytes , **E**:EM , **Hp**:HID proximity, **Hi**:HID iClass, **STA**:MiFare 4 & 7 bytes cards,HID iClass(CSN), Singapore CEPAS,Sony Felica,,**EXBC**:barcode)
FA	Facial model
FLI	Fingerprint Model
FA/FLI-S	Facial / Fingerprint + Smartcard Model
Others	***Meaning***
SAM	Sample Unit
W4	Built-in WiFi/4G module (optional)
ICOM	Built-in SIP intercom (optional)
P	Built-in PoE module (optional)
a	All-key enable available for MiFare or HID iClass .e.g.M**a** or Hi**a** to support to read 3rd party's smart card.
Note: The device's built-in 26bit Wiegand Output is on demand basis .	

Table 2.Legend

2.8.2. EXAMPLE

Model Number	Description
AT-1k-PC	Pin + Camera Model (up to 1,000 users)
AT-3k-SM	Smartcard Model (ACTAtek Mifare) (up to 3,000 users)
AT-3k-STA-C	Smartcard model (MiFare 4&7 bytes,HID iClass,CEPAS,Felica) + Camera (up to 3,000 users)
AT-1K-FA-FSMa	Facial model +Smartcard model(Open MiFare 4 bytes)+Camera(up to 1,000 users)
AT-1k-FSMa-C	Fingerprint Model (FLI)+ Smartcard Model (Open Mifare) + Camera (up to 1,000 users)
AT-1k-FLI-SHp-C-P	Fingerprint Model (FLI)+ Smartcard Model (HID prox.) + Camera +PoE (up to 1,000 users)

Table 3.Example

2.9. Standard Fingerprint / Smart Card/Facial Models:

Features	Fingerprint ONLY	Smartcard ONLY	Facial/ Fingerprint + Smart Card	Facial ONLY
Seven-Finger Enrollment	√	-	√	-
Built-in Smart Card Reader	-	√	√	-
Built-in Web and Database Server	√			
Built-in IP Video Camera	Optional	Optional	√	√
Static IP Address Assignment	√			
Support existing DHCP server	√			
Operating Temperature	-20C-60C			
Nand Flash Memory	4GB/8GB			
Maximum Users	1K users(default) to 100,000(maximum, depending on the model, on-request only)			
Maximum Auto-Match Users (1:N)	Up to 20,000 users	-	Up to 20,000 users	Up to 50,000 users
Maximum event logs stored	10K(default) to 1,000K (maximum)			
Maximum Photos stored	3,500 (maximum)			
Computers Supported	iOs / Windows 10 or above/ Unix / Linux Machines / Android			

Database Interface Support	ODBC / JDBC
Encryption	SSL/TLS 1.3
Multilingual Support	√
Programming API	SOAP/REST
Reporting	√
SNMP(optional)	√
Product Weight / Gross Weight with power supply & packaging	432g/1.5kg
Replaceable Modules	CPU / Fingerprint / Smartcard / Keypad/CAMERA/WiFi/4G/PoE
External I/O board support	√
LCD Module	Color screen
Product Dimension	175 x 81 x 41 (mm)
Weatherproof Casing	√
Expansion	RS-232 /Door strike#1/Door switch/alarm/bell/ RS-485(shared wiegand output)/12VDC output
Wiegand Output (standard 26bit)	√
Network Interface	1,000 BaseT Ethernet (Built-in) / WIFI IEEE 802.11 a/b/g/n/ac, with 2.4G/5G (optional)
Safety Standard	CE, FCC, SASO
Case	IP65fluid-ingress, dust, salt, fog, protection,IK10

Table 4.Standard Fingerprint and Smartcard Models

2.10. Warranty:

Please fill in the Warranty Card once you received the units. For the warranty to be valid, Warranty Card can be mailed or e-mailed or registered at our support website after you received your ACTA4. 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 ACTA4™ comes with the following, if anything is missing, please contact your dealer or us at support@actatek.com .

- ACTA4 Unit
- 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)

- Power Cord [according to Country Specification]

2.11. Setup Requirements

You can use any web-browser on any PC or Smart Phones. The ACTA4 devices are platform independent.

2.11.1. Operating System (For access via Corporate Network)

- Windows 10 or above version
- Linux Machines
- Unix Machine
- iOS
- Android

2.11.2. Network Interface

- 1,000 BaseT Ethernet (built-in)
- RJ45 Cabling for Network Connectivity.
- WIFI: IEEE 802.11 a/b/g/n/ac, with 2.4G/5G (Please refer to **Appendix K &L** for more information about ACTA4 WiFi setup.)
- Straight Network Cable (White/Blue cable, to connect to your corporate network via Switch)
- Crossover Network Cable (Black cable, to connect directly to your PC/laptop)

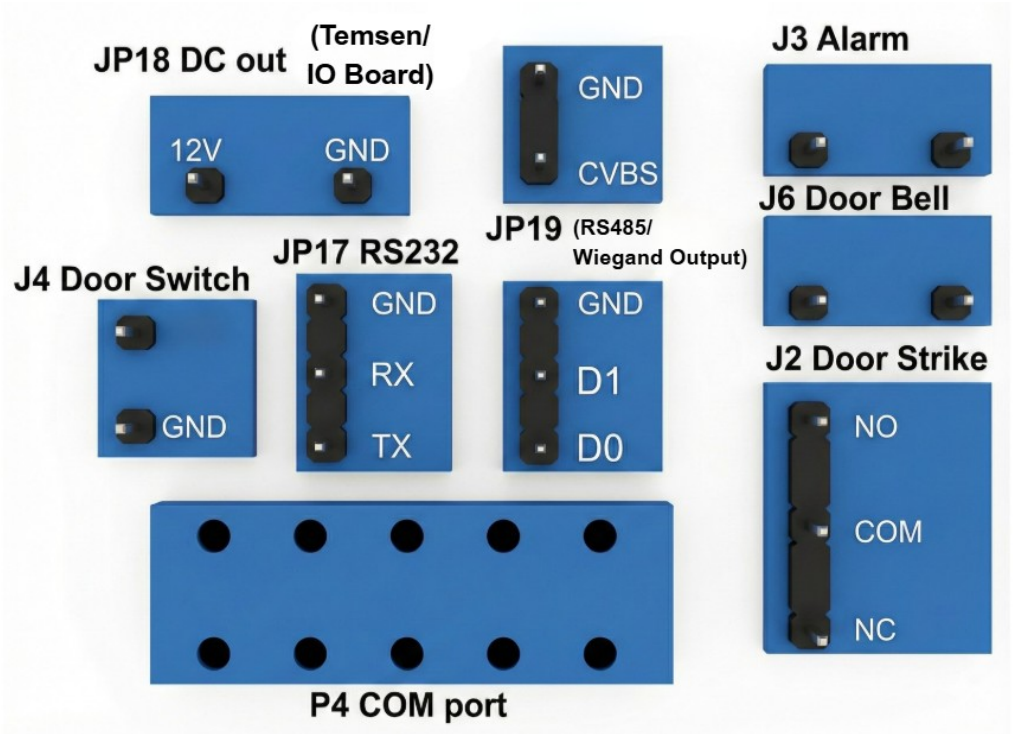
2.11.3. Power Requirements

- 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 ACTA4, failing to do so will void the warranty.

Chapter 3. ACTA4 Structure and Connections

3.1. *ACTA4™ Internal Structure and Connections*

ACTA4 back panel



3.2. Connection Details:

3.2.1. JP18

- Reserved for DC output to ACTAtek IO board /ACTAtek Temsen

3.2.2. JP20 *(* for the old ACTAtek CMOS model supports only)*

- Used for analog 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 26bit Wiegand output / RS485 (shared)

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

ACTA4 ™ 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

Features	Technical Specification
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

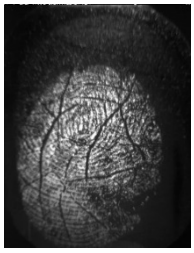
Table 5.Technical Information

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.

500dpi optical Fingerprint scanner

Fingerprint Core.

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

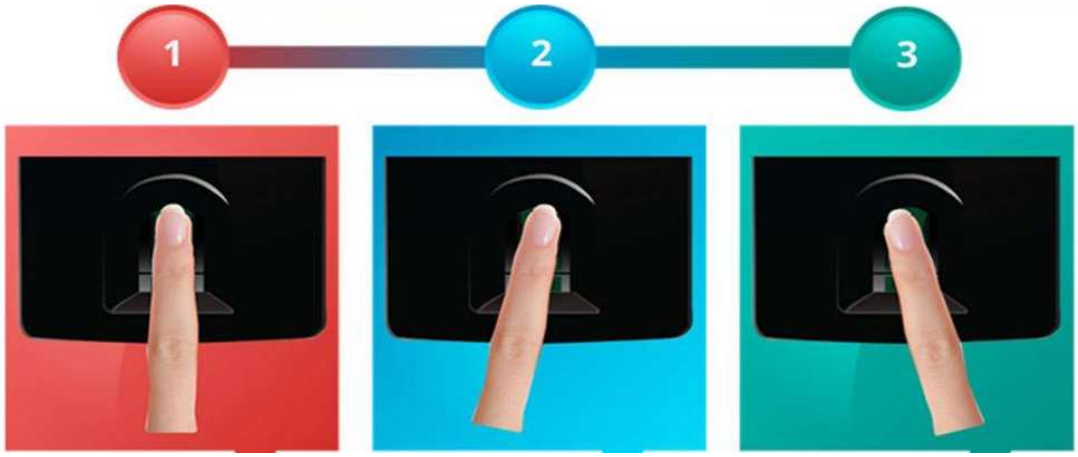
Make sure the fingerprint image captured is of the core of the finger presented. A fingerprint core is a point located within the innermost recurring ridge of any given finger.

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.

Once done the FP enrollment, please access the device few times to verify the successful enrollment

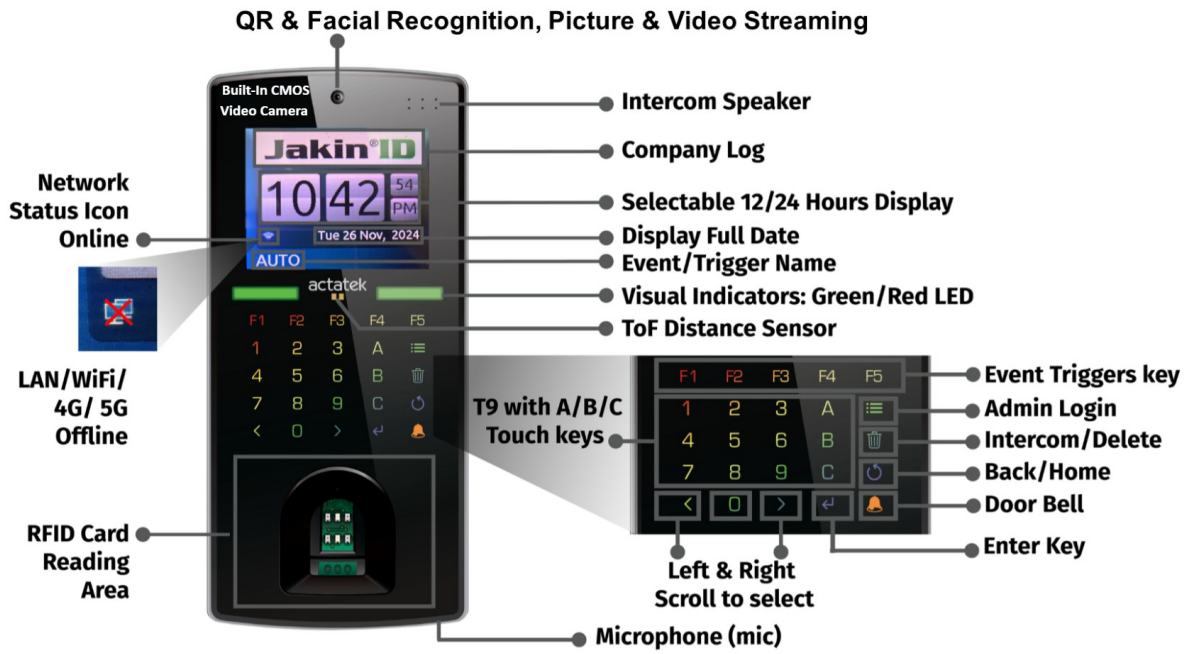
If you have any questions regarding the above FingerPrint enrollment procedure, you can e-mail us at support@actatek.com or check with the sales agent.

Chapter 5. ACTA4 Introduction

5.1. ACTA4 Introduction

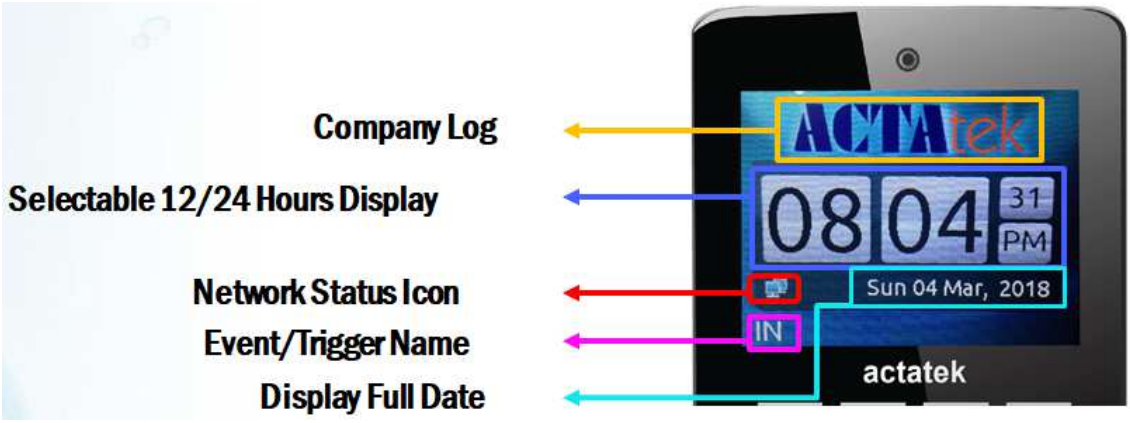
To begin operation of your ACTA4™, you must make sure it is connected to a 12V DC Power supply with the network cable securely attached to the port. Once your unit is powered up, the following screen should appear, the ACTAtek logo, the system clock, the Trigger should appear in the right corner, and 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.

ACTAtek Terminal GUI (standby mode) & Touch keypad



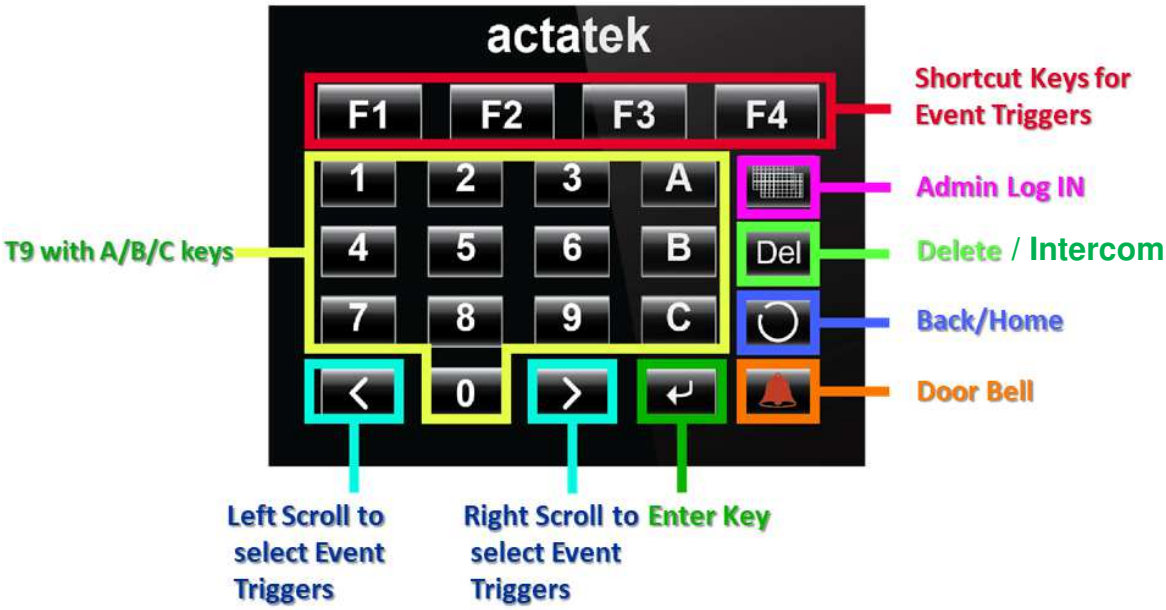
5.2. LCD Module

The Standby Screen displayed when the ACTA4™ 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 ACTA4 ™ Admin System

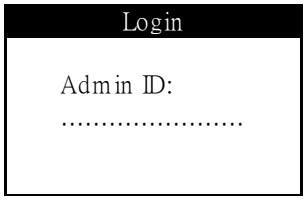
There are two ways for a Super Administrator to log in to the ACTA4 system, one is by fingerprint, and the other is by password.

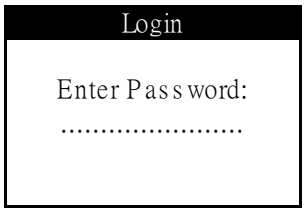
Logging in via Password:

- Press the [Admin Login] menu button on the keypad of your ACTA4 unit.
- The system will prompt for the Admin ID. Please enter the default one: 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 Login] menu button on the keypad of your ACTA4 unit.
- The system will prompt for the Admin ID. Please enter the default one: 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.





- Once logged into the system, a number of different actions can be performed, ranging from:
- Adding New Users via Face/ 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:

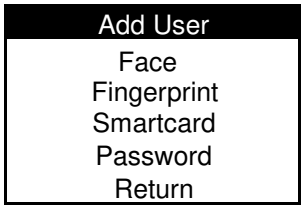
The first thing to do with the unit is to change the Administrator ID & password, to do so:

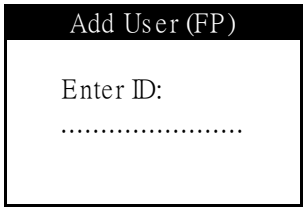
1. Log in to the web interface using a web browser. (Make sure the ACTA4™ is connected to the network). The device's default IP address is http://192.168.1.100/
2. Default Admin ID: **A999**, Default Password: **1**, **Super Administrator**, and click OK
3. Go to "View User List", click on the ID "A999".
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

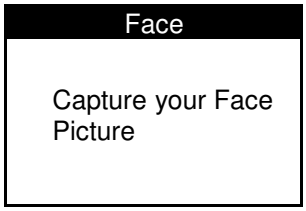
6.2.1. Adding A New User via Face

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





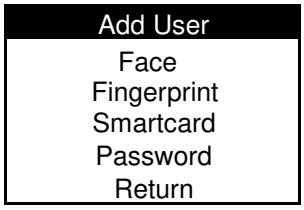
- Press Enter/Return
- Press Previous/Next until “Face” is Highlighted
- Press Enter/Return
- Enter the ID for the new user, e.g. AB01 (minimum 3 characters)
- Press Enter/Return

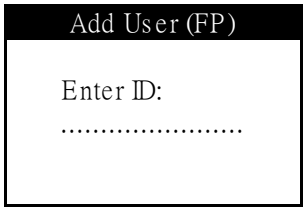


- After successfully captured your face picture, the message “User Added” will be displayed.
- Press Enter/Return to add another user, or Press the Menu button to go back to the Administrator Menu Screen, or press Back twice to exit from the system.

6.2.2. 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.

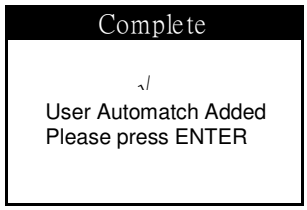




- Press Enter/Return

- 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

- 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.

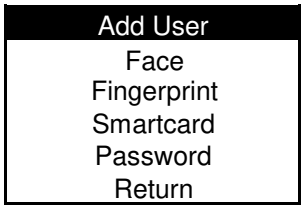


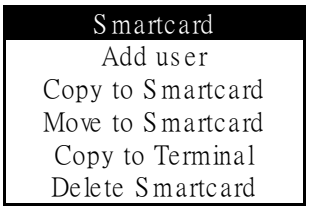
- After successful enrollment of the third fingerprint, the message “User Automatch Added” will be displayed.
- Press Enter/Return to add another user, or Press the Menu button to go back to the Administrator Menu Screen, or press Back twice to exit from the system.

Note: The User’s Auto-Match will automatically enable after FinerPrint enrollment

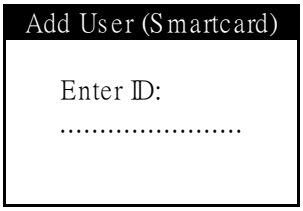
6.2.3. Adding A New User via Smart Card

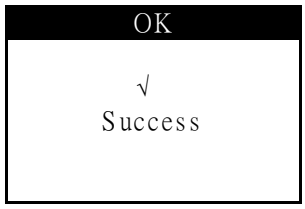
- After successfully entering the Administrator Menu, select the first icon on the top left of the screen, which is for Adding A New User.





- 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'

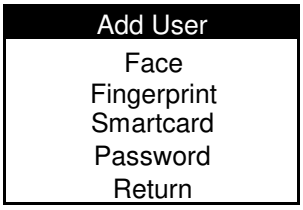


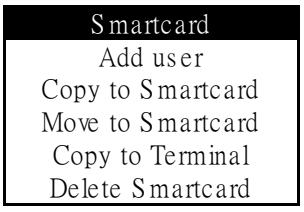


- Place the smart card over the bottom of the front case area.
- If successful, the write progress will be completed and "Success" will be displayed.

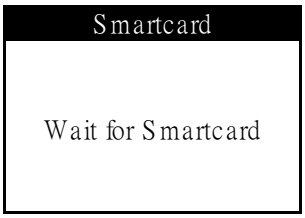
6.2.4. Deleting A Smart card user

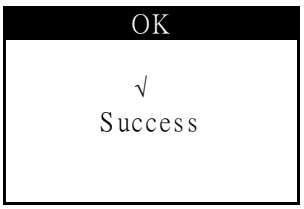
- After successfully entering the Administrator Menu, select the first icon on the top left of the screen, which is for Adding A New User.





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



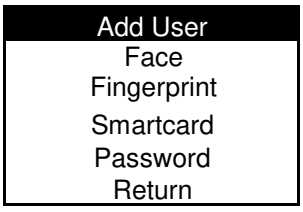


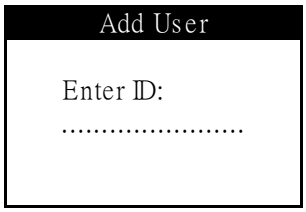
- Place the smart card over the scanner.
- If successful, the delete progress will be completed and "Success" will be displayed. The card will then be available for use for another user.

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

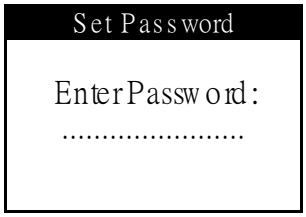
6.2.5. Adding A New User via Password

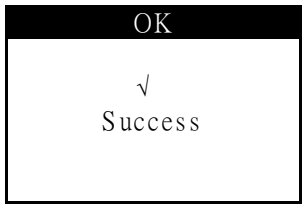
- After successfully entering the Administrator Menu, select the first icon on the top left of the screen, which is for adding a New User.
- Press Enter/Return





- 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





- 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.

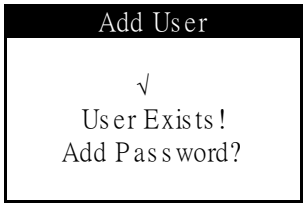
6.3. Error Messages

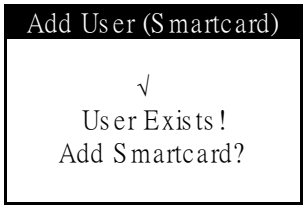
Beware Of..

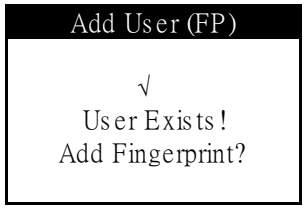
A “Bad Quality” warning will be displayed if the fingerprint enrolled is not of acceptable quality by the system.

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 overwrite users, you can press Enter/Return or press Back to cease any overwrite, and re-enter a unique user ID.
A999 cannot be used as a new ID since it is the default system administrator ID.

1. No User Record

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

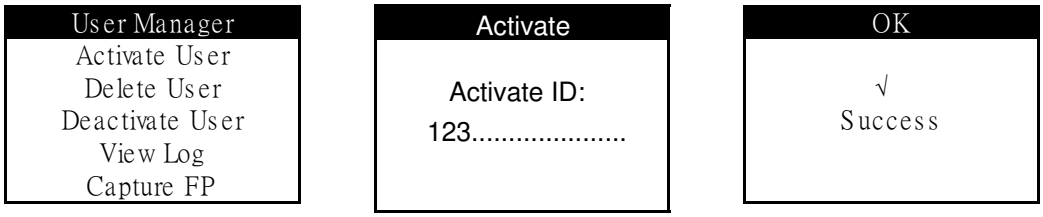
2. Unauthorized

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

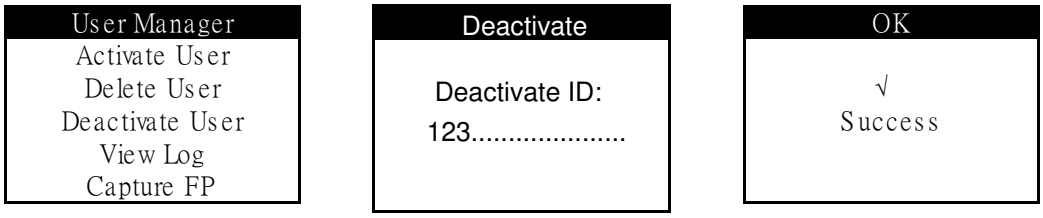
- After enrolling a few users into the system, you can manage them with the User Management option under the Administrator Menu.
- Select the second icon on the top left of the screen, which is for User Management.
- To activate a user, press the Previous or Next buttons until “Activate User” has been 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.



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

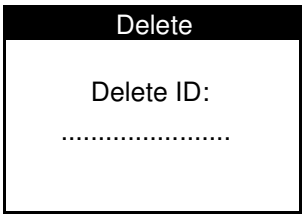
- After enrolling a few users into the system, you can manage them with the User Management option under the Administrator Menu.
- Select the second icon on the top left of the screen, which is for User Management.
- To deactivate a user, Press the Previous or Next buttons until “Deactivate User” has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

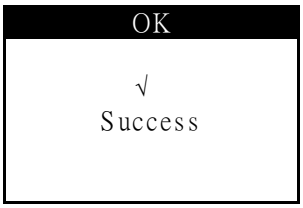


- If the user exists, and is successfully deactivated, the above screen will be displayed.
- Press Enter/Return to deactivate another user, or Press the Menu button to go back to the Administrator Menu Screen, or press Back twice to exit from the system.

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





- 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.*

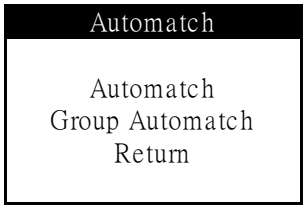
6.5. Auto Match

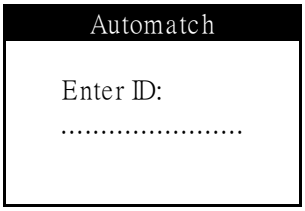
Auto Match – Enable/Disable

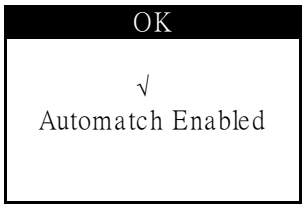
After enrolling users into the system via FingerPrint. Auto Match may be enabled for individual users. The primary function of Auto Match is to allow users to access the system without inputting their ID first. All they need to do to gain access is to place their fingers on the scanner and let the ACTA4™ 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.



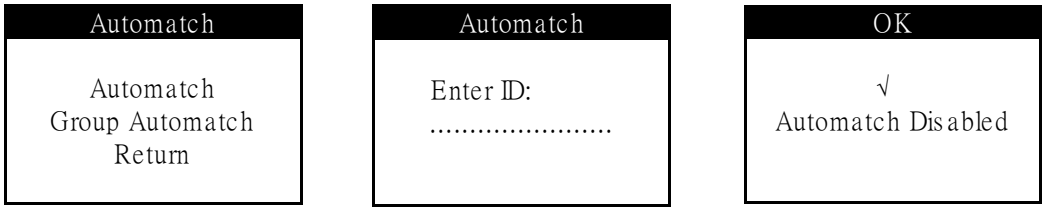




- Enter the ID of the user for whom Auto match/Group Auto match is being enabled, e.g. 123.
- Press 'Enter/Return'.
- If the user exists in the system, and their Auto Match function was not previously enabled, the message "Automatch Enabled!" will be displayed.
- Press 'Enter/Return' to enable Auto Match 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.



- Enter the ID of the user for whom Auto Match /Group 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.

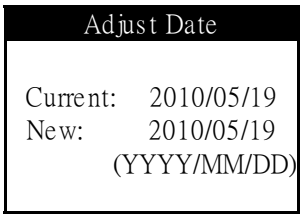
6.6. Date & Time

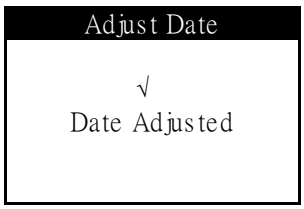
Date & Time Function

ACTA4™ 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.

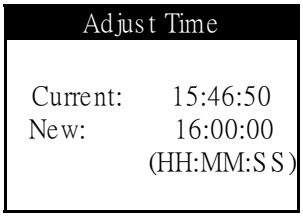


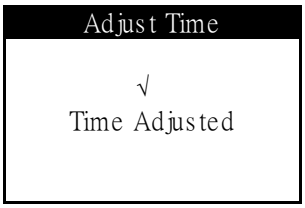


- Press 'Enter/Return' to modify the Time or other settings, or Press the 'Menu' button to go back to the Administrator Menu Screen, or press 'Back' twice to exit from the system.

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.





- 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.

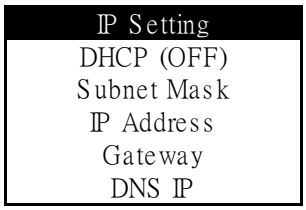
6.7. IP Settings

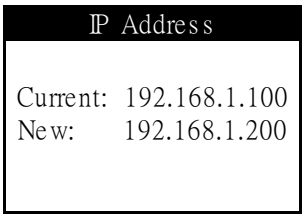
IP Settings Function

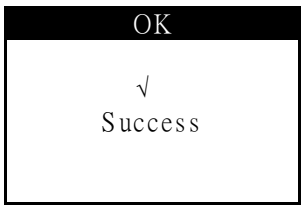
ACTA4™ is a web-based system, and works similarly as a network appliance. Having say that, it has its own IP Address assignment, either by using Dynamic or Static Assignment. This will allow the administrator to access the device Web UI via any browsers such as Internet Explorer, Firefox, or Chrome etc. 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 ACTA4™ 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.





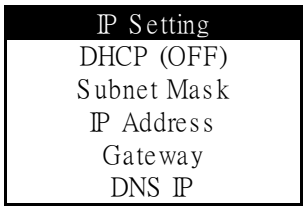


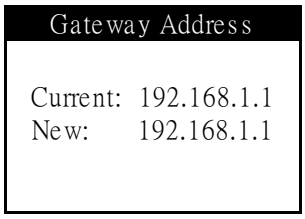
- Press 'Enter/Return' to modify other settings in the IP Settings option, or Press the 'Menu' button to go back to the Administrator Menu Screen, or press 'Back' twice to exit from the system.

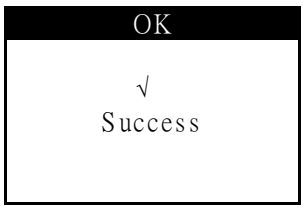
Note: For "Scan WIFI QR Code" setting, please refer to 'Appendix L' about ACTA4 WiFi setup for more information.

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.



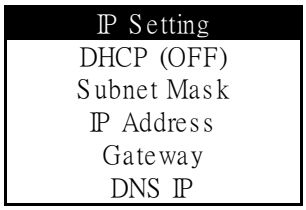


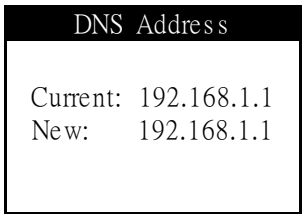


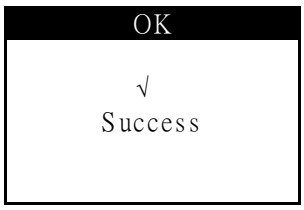
- Press 'Enter/Return' to modify other settings in the IP Settings option, or Press the 'Menu' button to go back to the Administrator Menu Screen, or press 'Back' twice to exit from the system.

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.





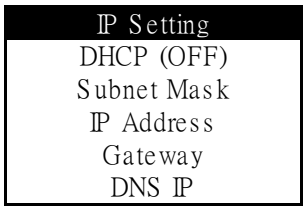


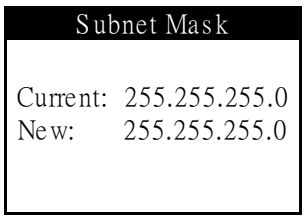
- Press ‘Enter/Return’ to modify other settings in the IP Settings option, or Press the ‘Menu’ button to go back to the Administrator Menu Screen, or press ‘Back’ twice to exit from the system.

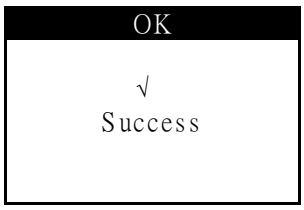
***Note: DNS IP is used to resolve Domain Names to IP Address and vice versa.**

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 .







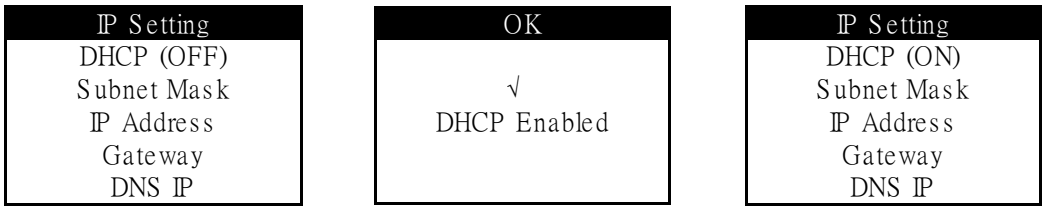
- Press ‘Enter/Return’ to modify other settings in the IP Settings option, or Press the ‘Menu’ button to go back to the Administrator Menu Screen, or press ‘Back’ twice to exit from the system.

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.



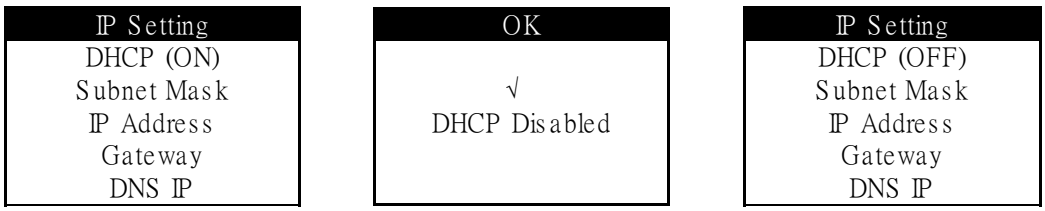
- Press 'Enter/Return'.
- The Current status of the DHCP will be displayed, if it is "DHCP (OFF)", it will be enabled.

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'.



- 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

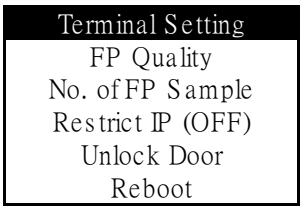
The terminal settings feature allows users to set the ACTA4™ in a multi-user environment. Moreover, the Terminal Settings option can allow users to set the Security Level from High to Low, with High Fingerprint Security allowing for maximum minutiae to be accounted for during authentication. The Low 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.

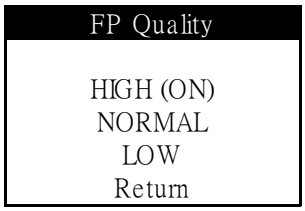
Note:

- ***For "Master/Client setup" setting, please refer to Appendix I for more information.***
- ***For "FACE CAPTURE" setting, it is reserved for the troubleshooting of User Facial recognition.***

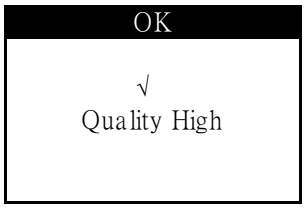
6.8.1.1. Fingerprint Security Level Settings

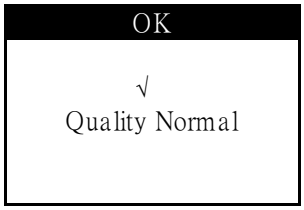
- Select the second icon on the bottom left of the screen, which is for Terminal Settings.
- Use the Previous / Next button until "FP Quality" is highlighted.
- Press Enter/Return

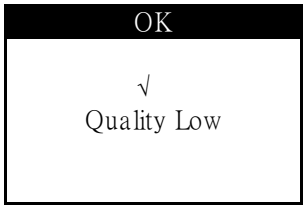




- The three options to select from include: High, Normal or Low. Each of which will give you the following display messages:



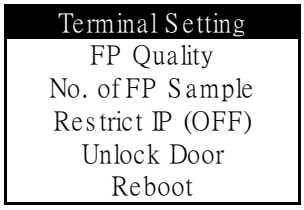


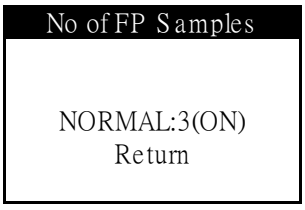


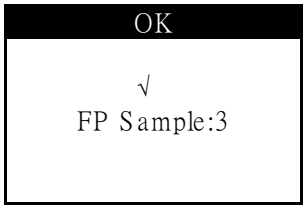
- Press Enter/Return to modify other settings in the Terminal Settings option, or Press the Menu button to go back to the Administrator Menu Screen, or press Back twice to exit from the system.

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



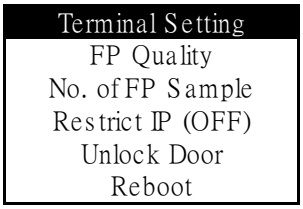


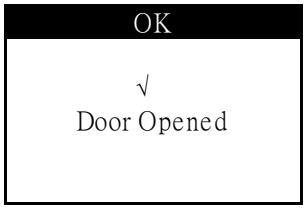


- The three options to select from include: Normal:3 (default). Once selected, the system will take that number of FP templates during enrollment of new users.
- Select one and press 'Enter/Return' to save settings.
- Press Enter/Return to modify other settings in the Terminal Settings option, or Press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

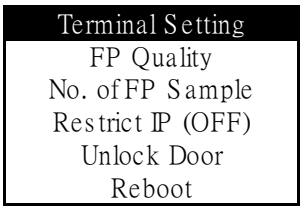
6.8.4. Enable/Disable Face Spoof

- Use the Previous / Next button until “Enable/Disable Face Spoof” is highlighted.
- Press Enter/Return to enable or disable Face anti-spoof function.

Note:More [Anti-spoofing] methods can be selected from the device’s [Terminal Setup] webpage.

6.8.5. 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.
-



-

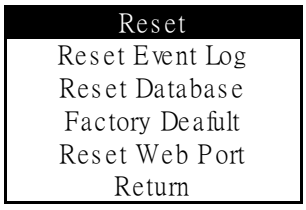
6.9. Reset

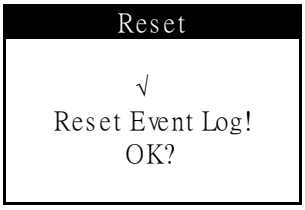
Reset Setting Function

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

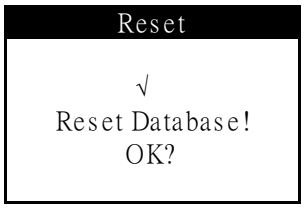




- If successful, a “Event Log Reset!” message will be displayed.
- Press Enter/Return to modify other settings in the Reset Setting option, or Press the Menu button to go back to the Administrator Menu Screen, or press Back twice to exit from the system.

6.9.2. Resetting the User Database

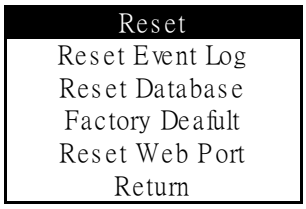
- Select the third icon on the bottom left of the screen, which is for Reset System.
- Use the Previous or Next button until “Reset Database” is selected
- Press Enter/Return

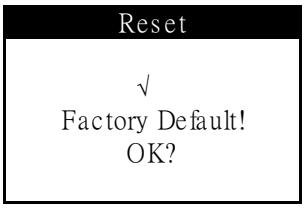


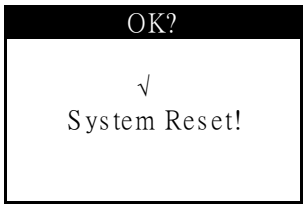
- If successful, a “Database Reset!” message will be displayed.
- Press Enter/Return to modify other settings in the Reset Setting option, or Press the Menu button to go back to the Administrator Menu Screen, or press Back twice to exit from the system.

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.

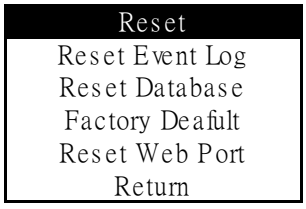


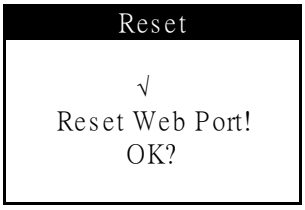




6.9.4. Web Port

- 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

ACTA4™ 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.

ACTA4™ 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

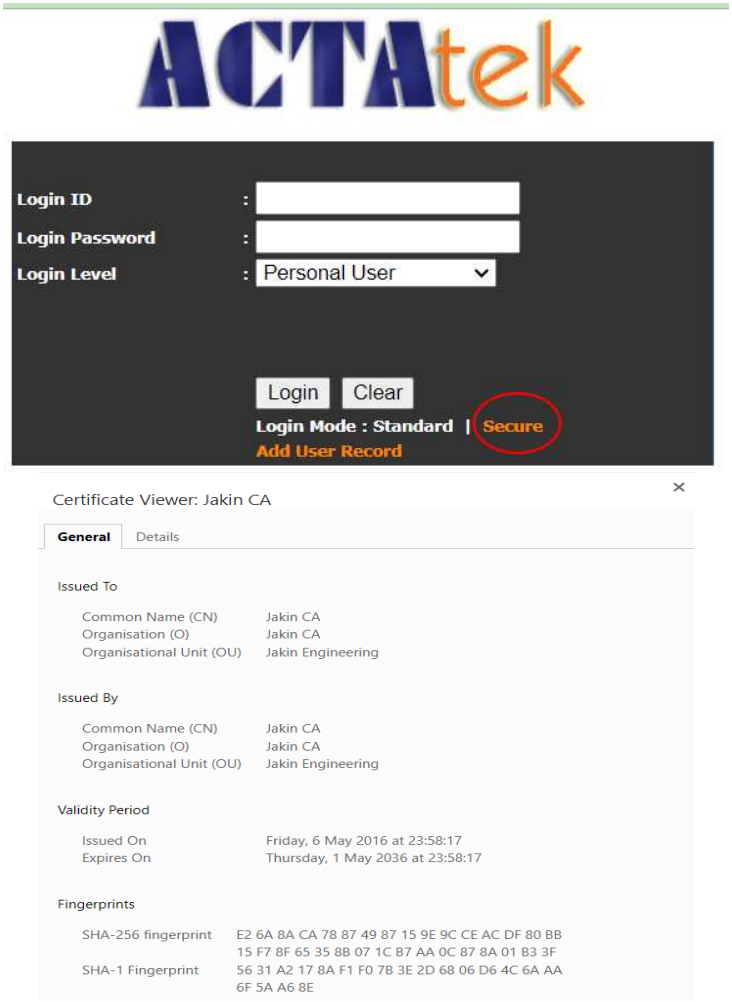
The network administrator is in charge of system configurations, such as, networking settings, terminal settings, clock setups, or password setups. Everything that involves technical knowing will be done by the network administrator. This role is usually assigned to a tech-savvy person, who is capable 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 ACTA4™ unit) is typed on the address bar of Edge or Chrome or any other web browser, the login page will appear. Click on "Secure" to login using secure TLS 1.3 data encryption, so that ALL the exchange of data is encrypted and secure.

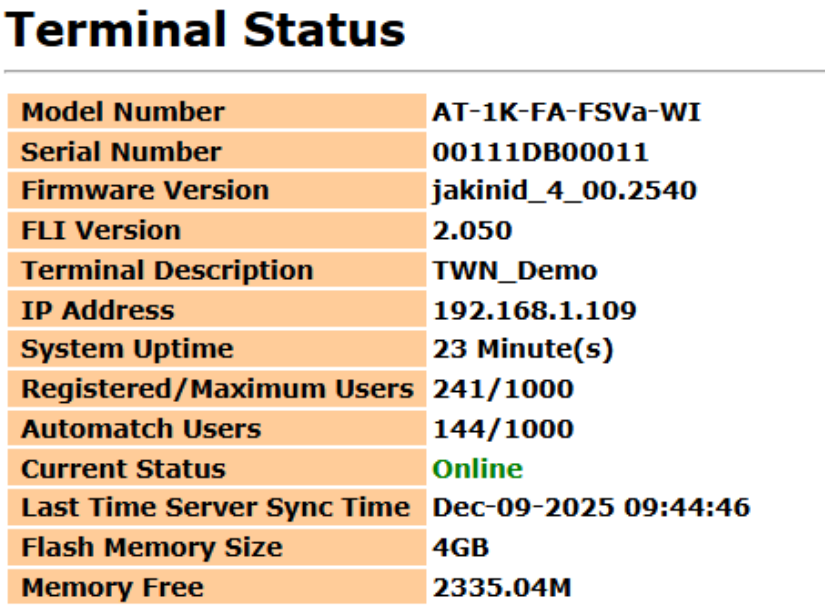


After selecting "Secure" login, the above screen will be displayed and to go on to login to view the web interface of ACTA4, select either "Accept this certificate permanently" or "Accept this certificate temporarily for this session". It is recommended to have the temporarily selected if you are not 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



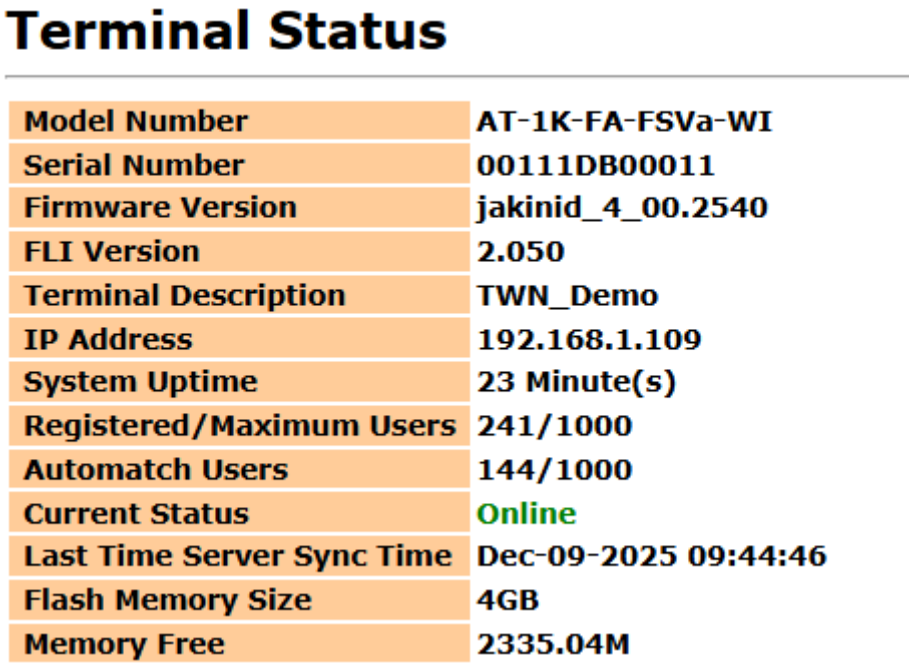
The first page displayed, as above, will be the same no matter which login is chosen. It will show a brief status of the terminal. The information displayed includes:

Feature	Description
Model Number	The Model Number of your ACTA4™ unit.
Serial Number	The Serial Number of your ACTA4™ unit.
Firmware Version	The software version installed in the unit.e.g.4_00.2540
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
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. -FLI mode: up to 20,000 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.



Terminal Status

Model Number	AT-1K-FA-FSVa-WI
Serial Number	00111DB00011
Firmware Version	jakinid_4_00.2540
FLI Version	2.050
Terminal Description	TWN_Demo
IP Address	192.168.1.109
System Uptime	23 Minute(s)
Registered/Maximum Users	241/1000
Automatch Users	144/1000
Current Status	Online
Last Time Server Sync Time	Dec-09-2025 09:44:46
Flash Memory Size	4GB
Memory Free	2335.04M

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
3. Add Record -To add user's time record from device's webpage.

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. Job Code -To setup the old Job Code after enable it at [Terminal Setup] page
4. 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. WiFi Setup -To setup ACTA4 WiFi connection (**See Appendix K**)
3. Mobile broadband -To setup ACTA4 4G connection **(See Appendix M)**
4. Intercom -To setup ACTA4 Intercom **(See Appendix J)**

5. Authentication / Log Setup - To setup the behavior of authentication log.
6. Terminal List - To view the list of terminals connected.
7. Master/Client or Access Client setup -To setup Master/Client function (Standalone mode)
   - To configure the ACTAtek to register with Access Manager Suite. (*Access Manager mode*)
8. Door Open Schedule - To view or modify the door opening schedule.
9. Bell Schedule - To view or modify the bell schedule period.
10. Terminal Clock - To view or modify the terminal clock settings.
11. External Devices - To connect external I/O board to the ACTA4 unit.
12. DDNS -To enable DDNS ,and the device can be accessible from Internet via signed up DDNS

8.1.5. Terminal

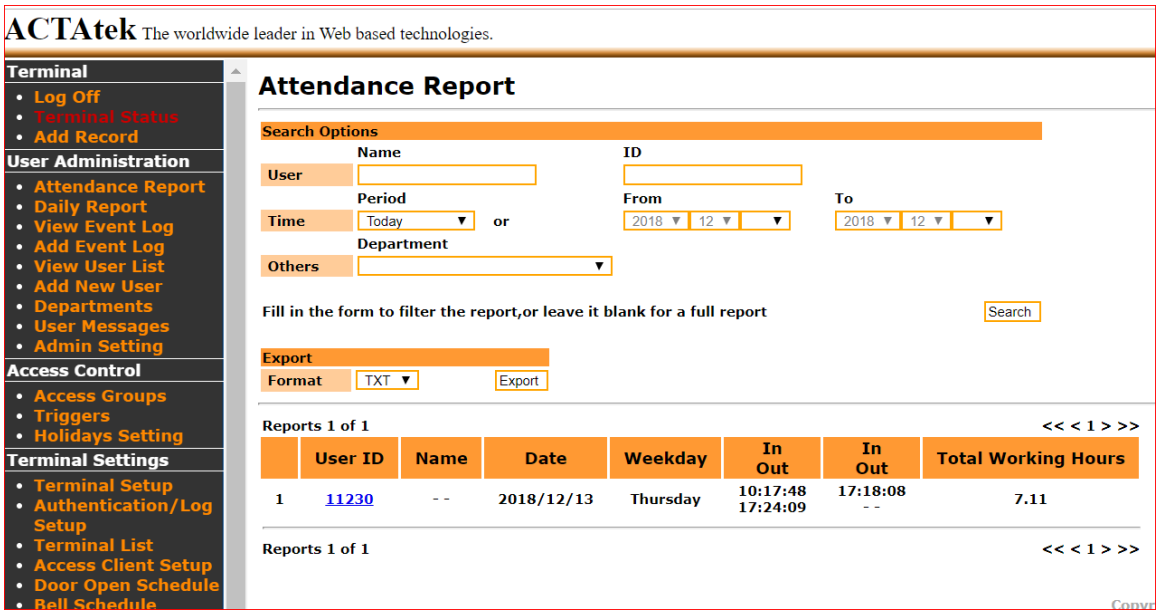
1. Cloud Storage Service - Google Drive Spreadsheet integration
2. SMS Service -To setup the SMS service
3. Alert Log -To setup which action gives out alert log
4. Syslog -To enable the remote system log
5. Backup System Data - To backup the system data.
6. Restore System Data -To restore the system data from a previous setting
7. Firmware Upgrade - To upgrade the firmware or patch files provided by 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 ACTA4™ 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:



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

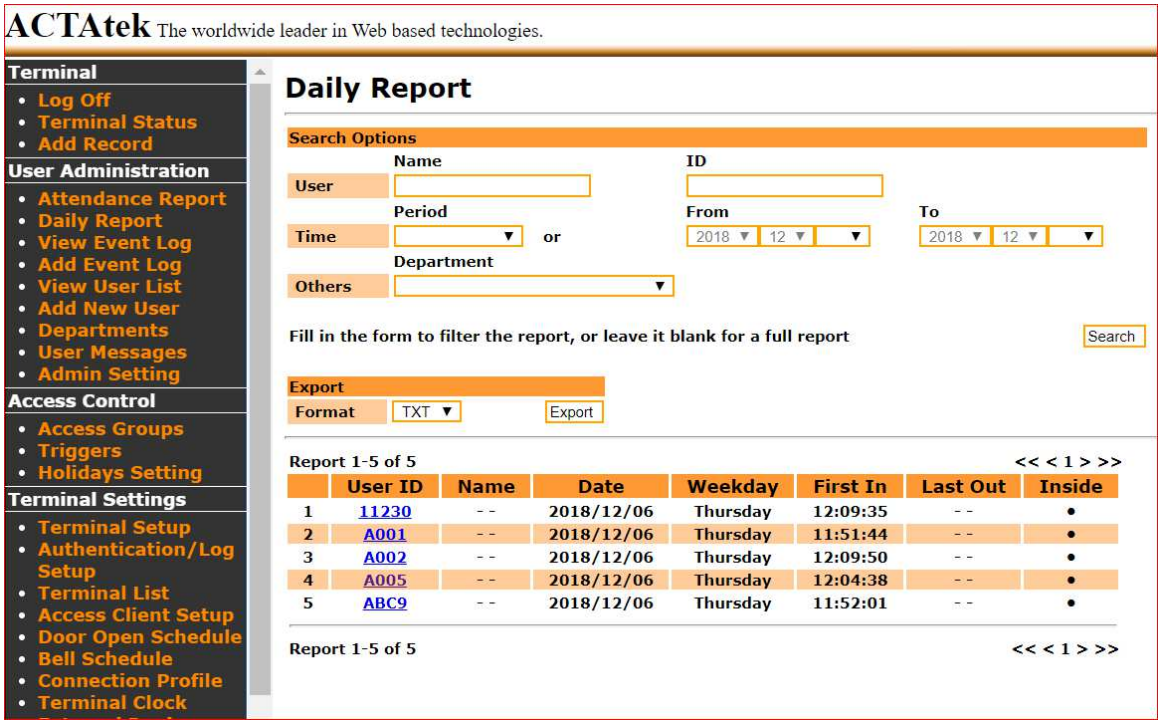
There are 4 different searching options available to view the Attendance Report which includes "Name", "User ID", "Fixed Period" or "Specific Range of Date" and "Department".

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.

8.2.2. *Daily report*

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



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)

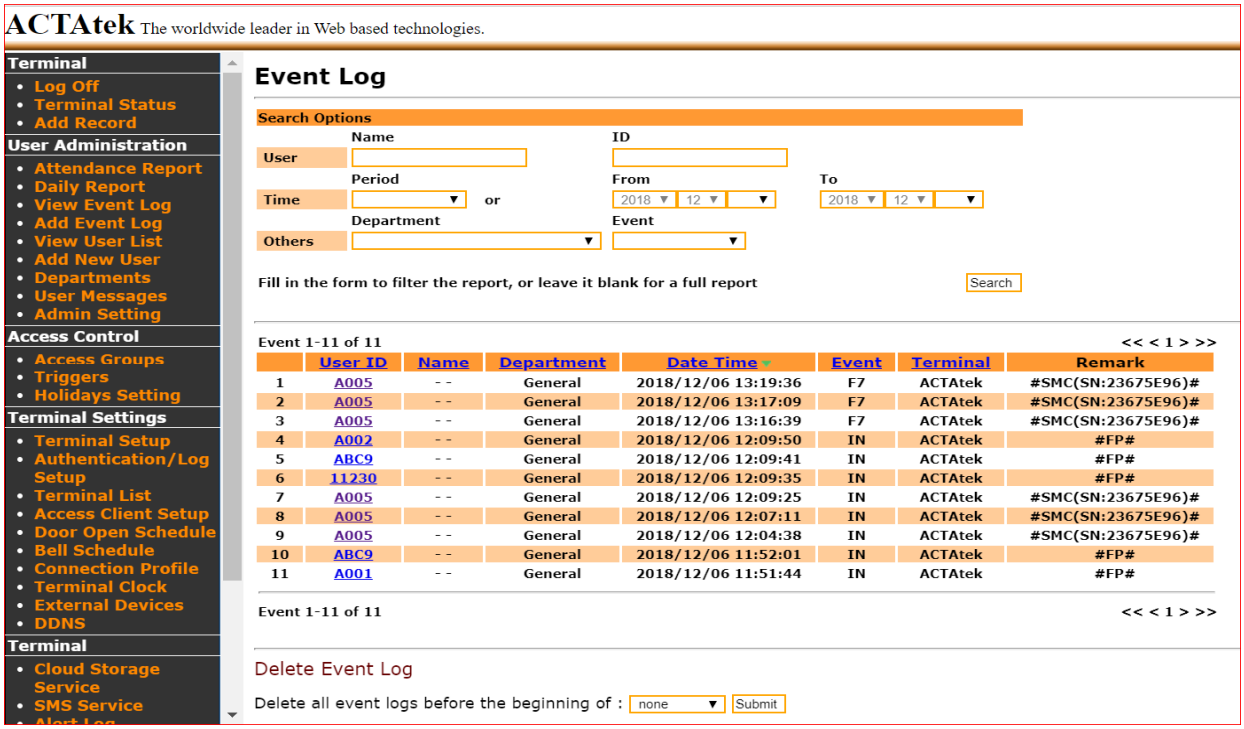
There are 4 different searching options available to view the Attendance Report which includes "Name", "User ID", "Fixed Period" or "Specific Range of Date" and "Department".

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 3rd party HRMS or Payroll company to import the data into their system.

8.2.3. *View Event Log*

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



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, FACE,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.

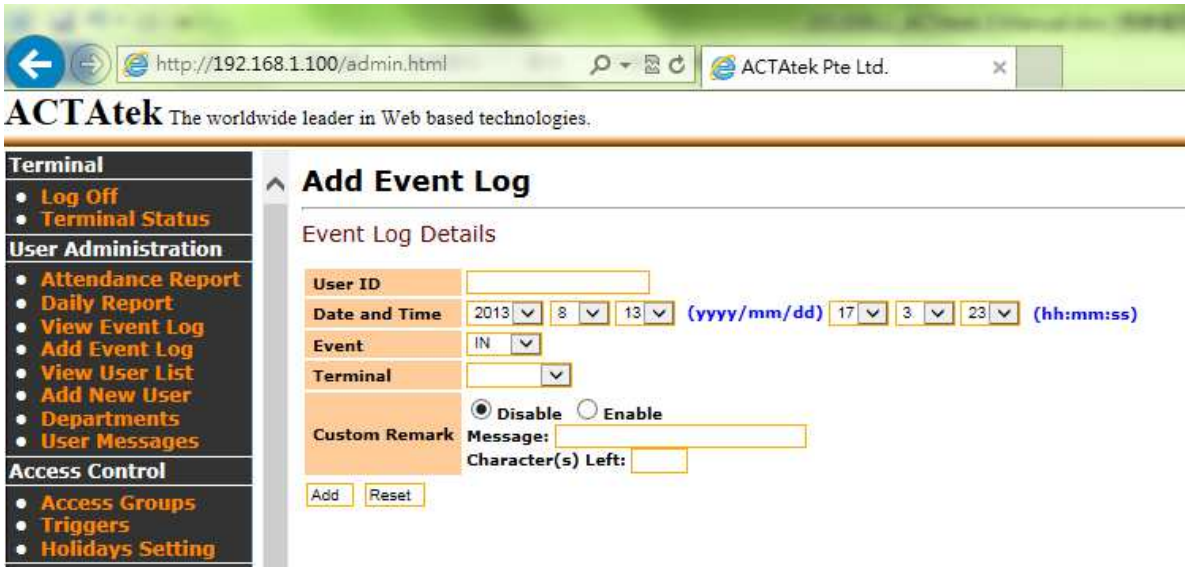
8.2.3.1. Deleting Event Logs

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”.

8.2.4. 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.



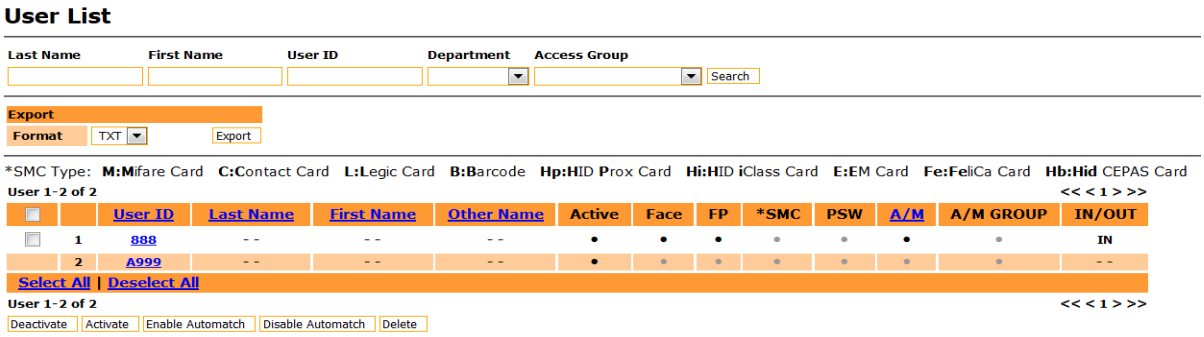
Select “Add Event Log” under User Administration from the left of your screen, and the above screen should be displayed.

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.

8.2.5. *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.



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”,”Face”,” FP”, “SMC”, “PSW”, “A/M” ,”A/M Group”, and “IN/OUT”.

Description of Information displayed:

Feature	Description
1. Active	The Status of the User: Black –Active , Grey - Inactive
2. Face	Whether Face is an available authentication option.
3. FP	Whether Fingerprint is an available authentication option.
4. SMC	Whether Smart Card is an available authentication option.
5. PSW	Whether Password / PIN is an available authentication option.
6. A/M	Whether Auto-match is an available authentication option.
7. A/M Group	Whether Auto-match Group is an available authentication option.
8. IN/OUT	Whether the user is currently In or Out of Premises.

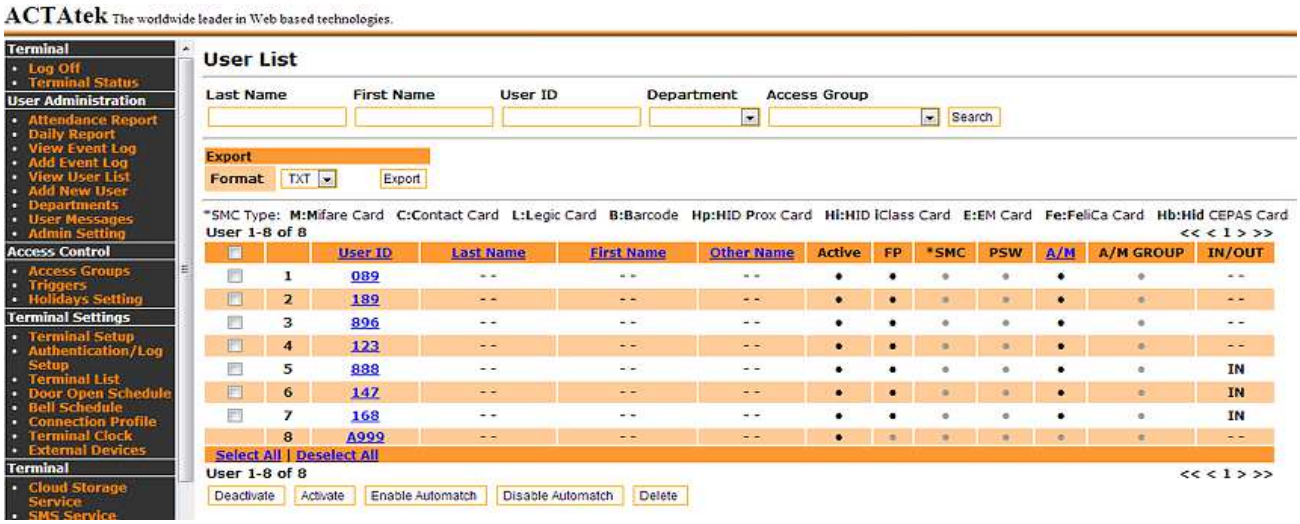
“Export”: You can export a list of registered users and their status into TXT/CSV file format.

8.2.5.1. 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.

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

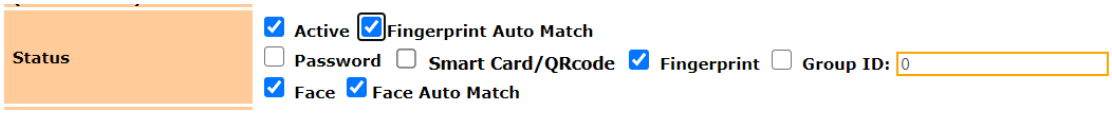
To delete users from the system, you can select the checkboxes on the left of the ID under User List. If all the users need to be deactivated/deleted/activated, click the “Select All” to check ALL boxes. To cancel the selection, click on “Deselect All”. Once selected, click the respective buttons at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



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.

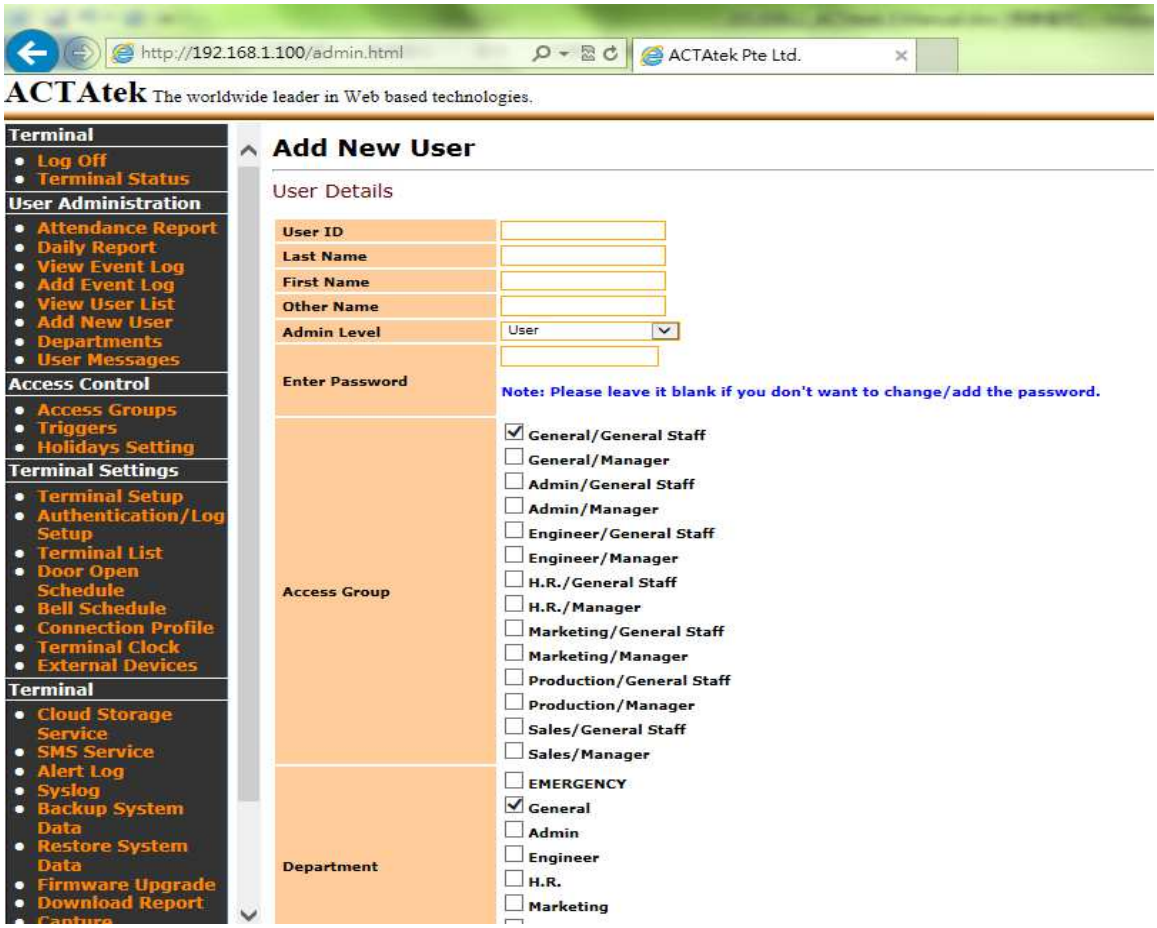


8.2.6. To Add New Users

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.

8.2.6.1. To Add A New User:

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



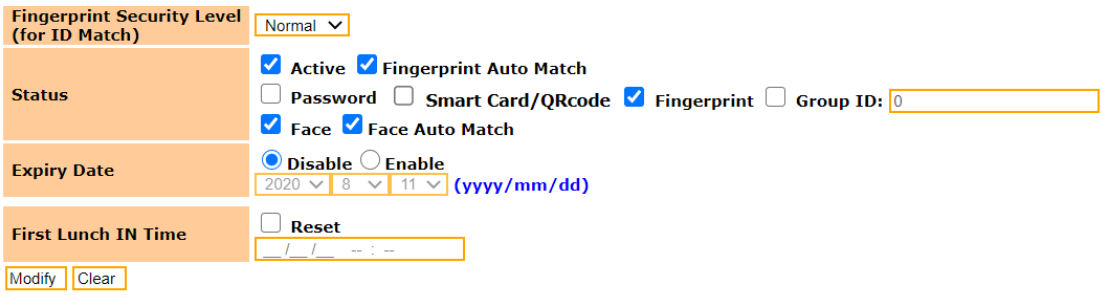
Enter the User ID, Last Name, First Name, Other Name, Admin Level and enter the password in the following field. Check the relevant boxes for the relevant Access Group, this will limit or give them access at different times or doors, depending on the configuration made.

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.

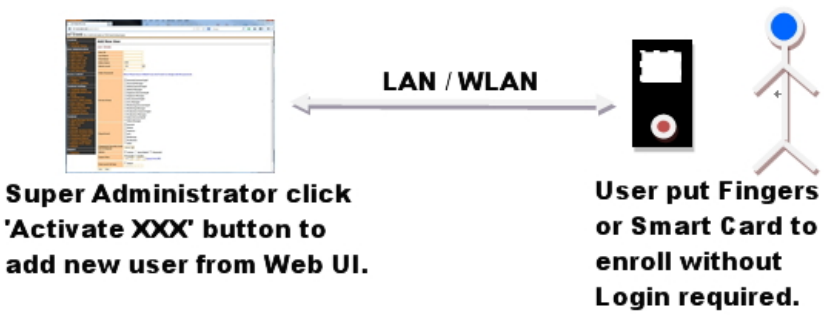
Select the status of the user, whether they can use Auto Match or Password, and you can set the expiry date of the user if any. After that, you can click “Add” to add the new user.

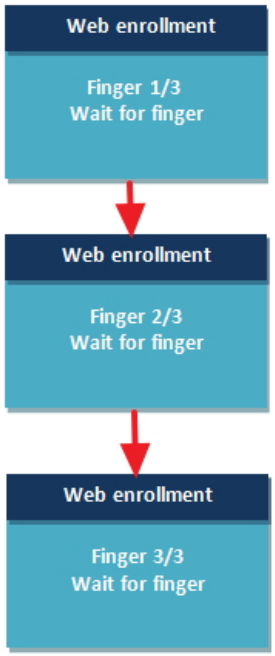
Note: Auto Match will be available when there is a FingerPrint enrolled already.

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



Note: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.





For FACE model device, the administrator can also remotely add Facial photo by choosing and uploading the User's JPEG file from the local drive and click on "Upload" button.

Once the User's facial photo file was uploaded to the device,the device will convert the photo file to the facial template for the facial recognition. Click Add button to finish adding the new FACE user.

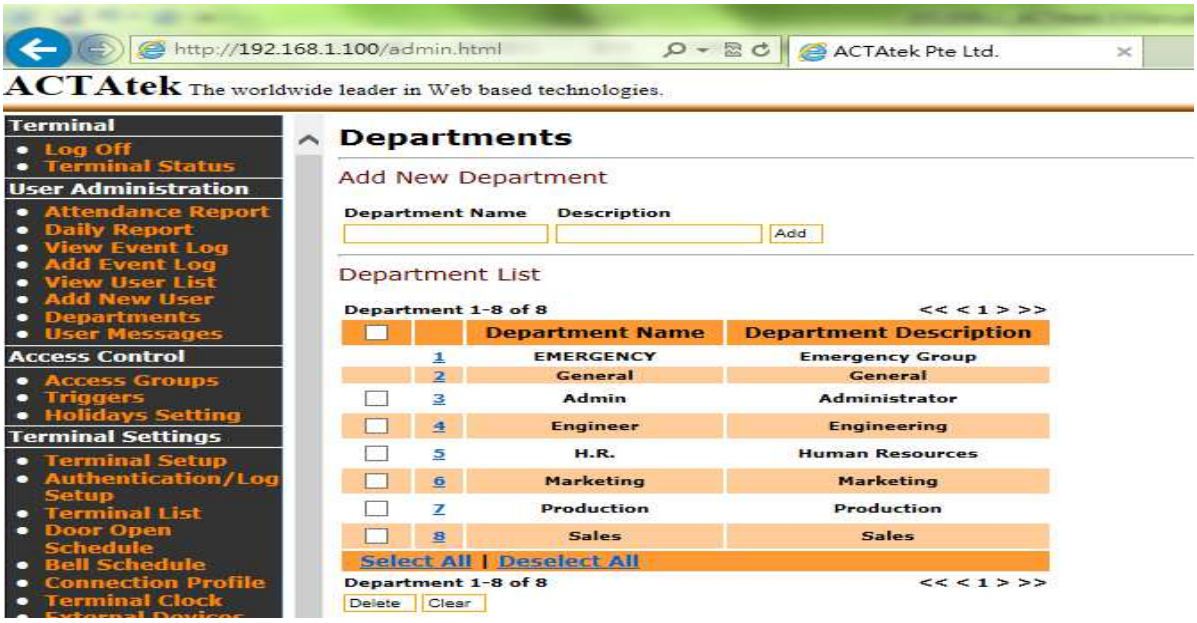
Note:Please make sure the User's JPEG file size is not larger than 1000*1000 pixels.

8.2.7. Departments

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

8.2.7.1. 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.



8.2.7.2. 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.

8.2.7.3. 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.**

8.2.8. 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 ACTA4™ unit.

8.2.8.1. 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 ACTA4 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.

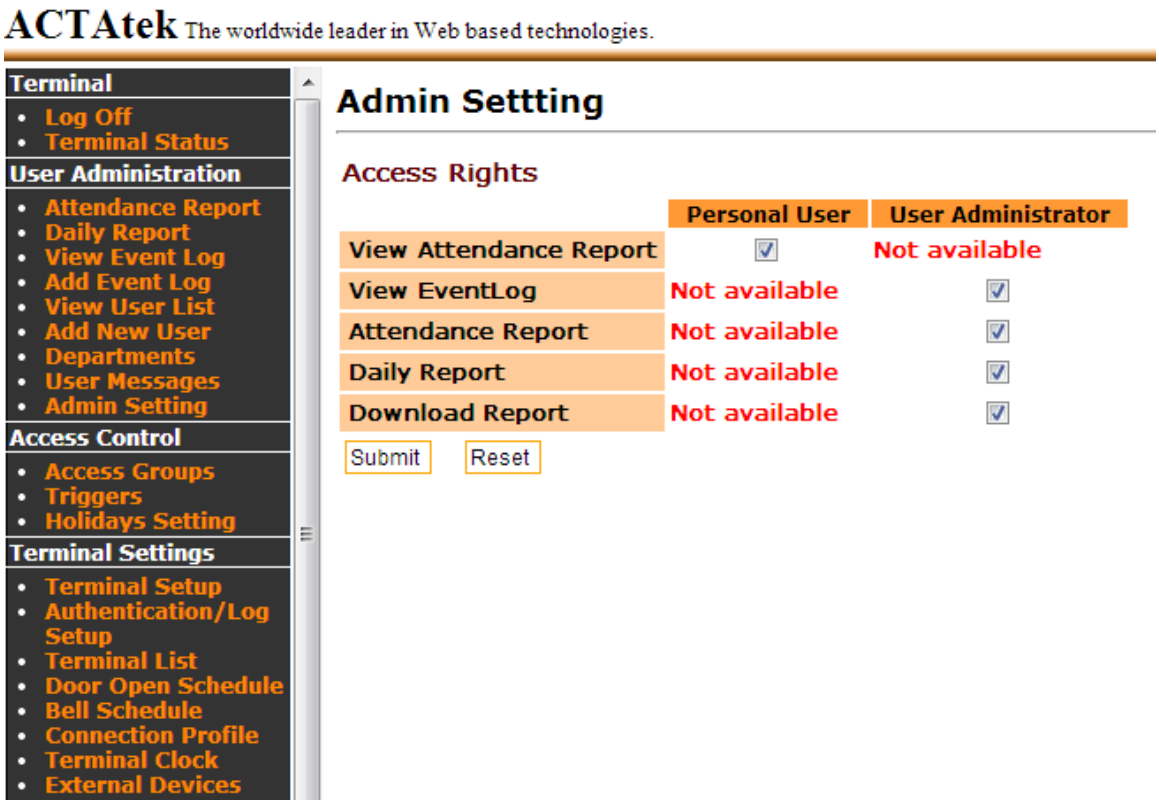
Note: You can enable "Delete the message after display once" if the user message will only displayed one time.

8.2.8.2. 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.

8.2.9. 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.



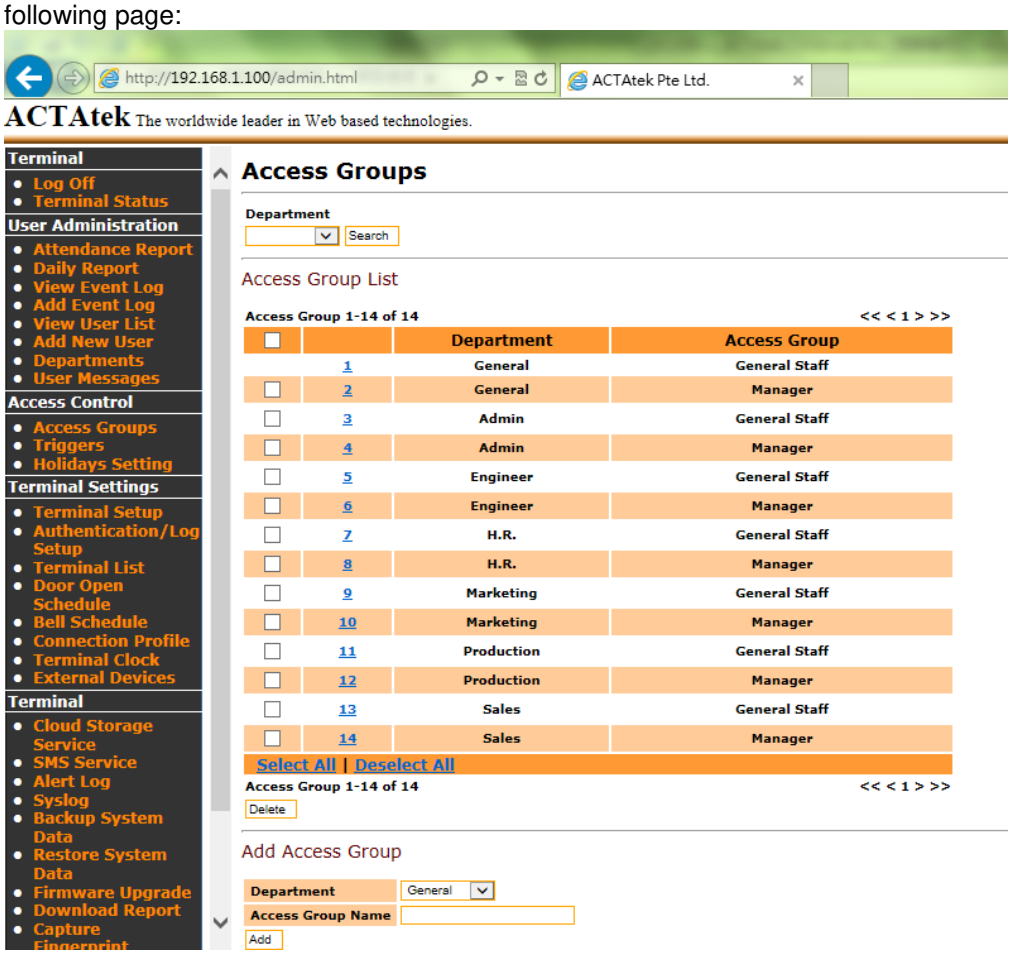
8.3. Access Control

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:



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

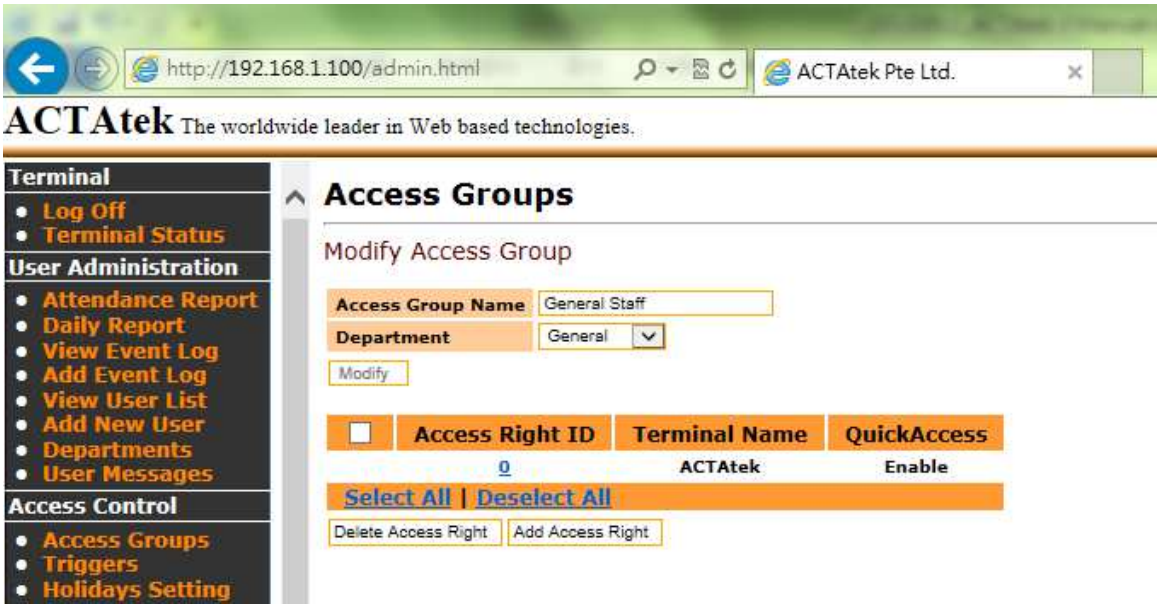
To Delete the Access Group(s), check the relevant box and click “Delete”, or use the “Select All” option to select ALL the access groups; or use the “Deselect All” option to clear the selection.

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.

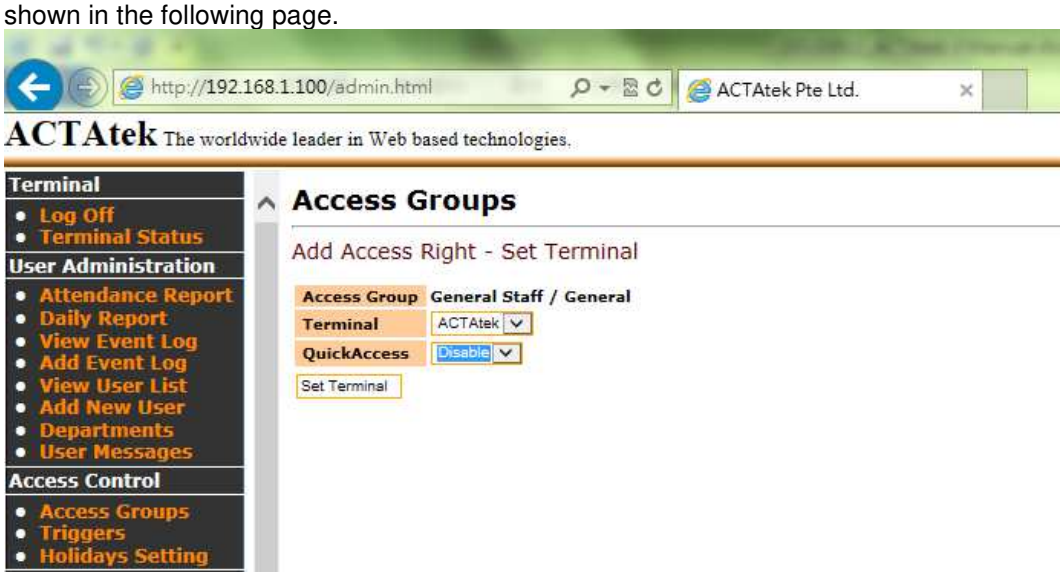


The top part displays the Access Group Name and associate Department. This can be modified by renaming the Access Group Name and/or assigning to a different Department.

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

8.3.1.4. To Add a New Access Right

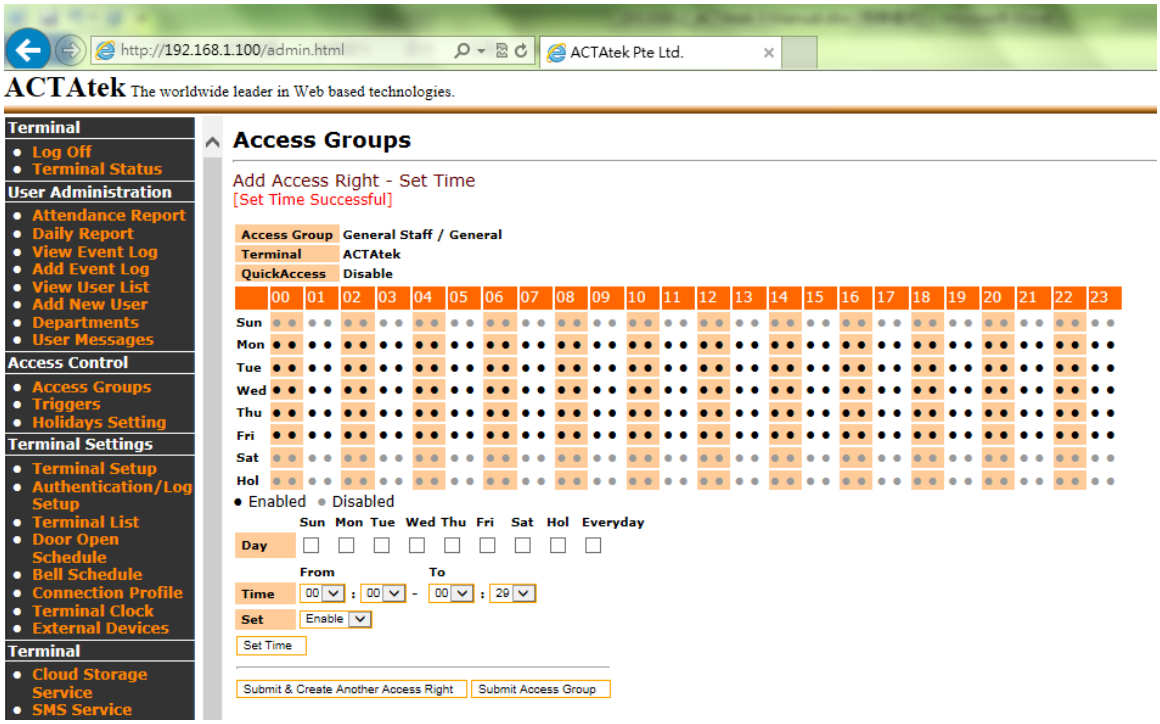
Click on “Add Access Right”. Select which terminal this access right is assigned to, and set whether Quick Access is enabled or disable. *(“Disable”: it can be used for dual access e.g.Smart Card plus FingerPrint to access the device.)* Click on “Set Terminal” for proceed, as shown in the following page.



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.



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”.

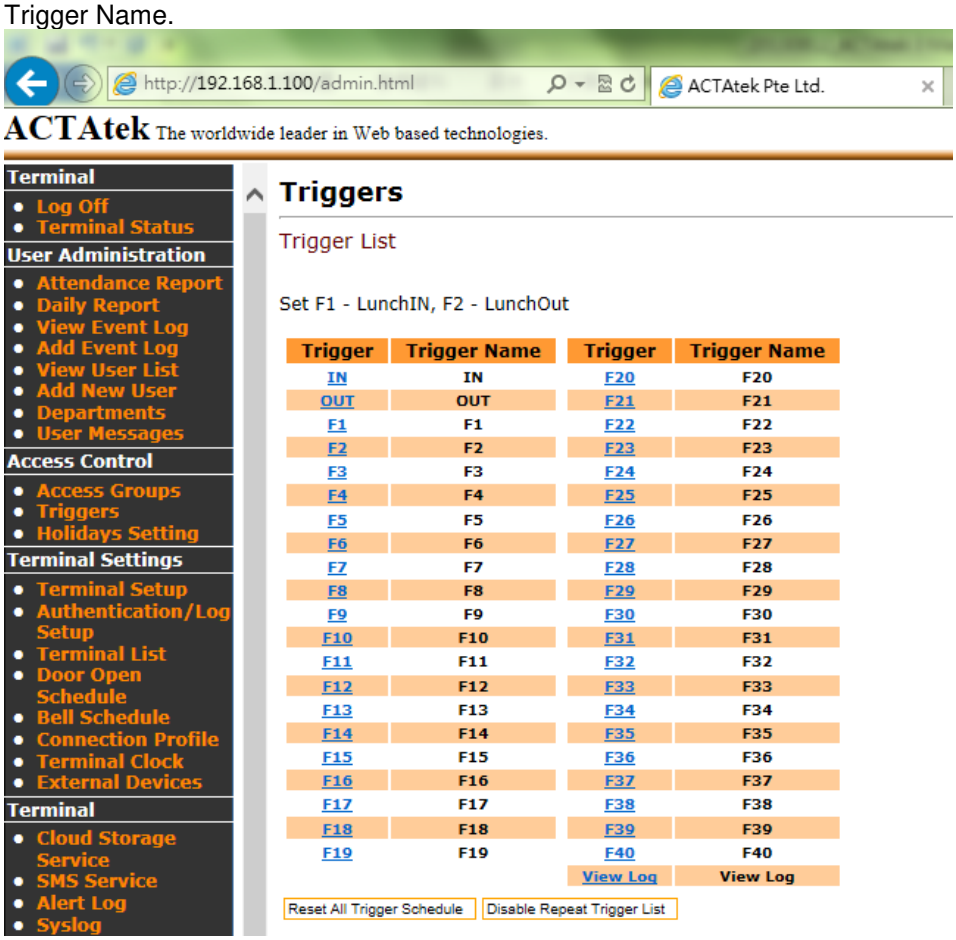
The information that can be modified includes:
Quick Access: -Choose to access the device using FingerPrint or Smart Card or PIN (Quick access: Enable) or dual access (Quick access: Disable)
The Access Time: -From which day and when does this Access Group is allow to access the terminal.

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.

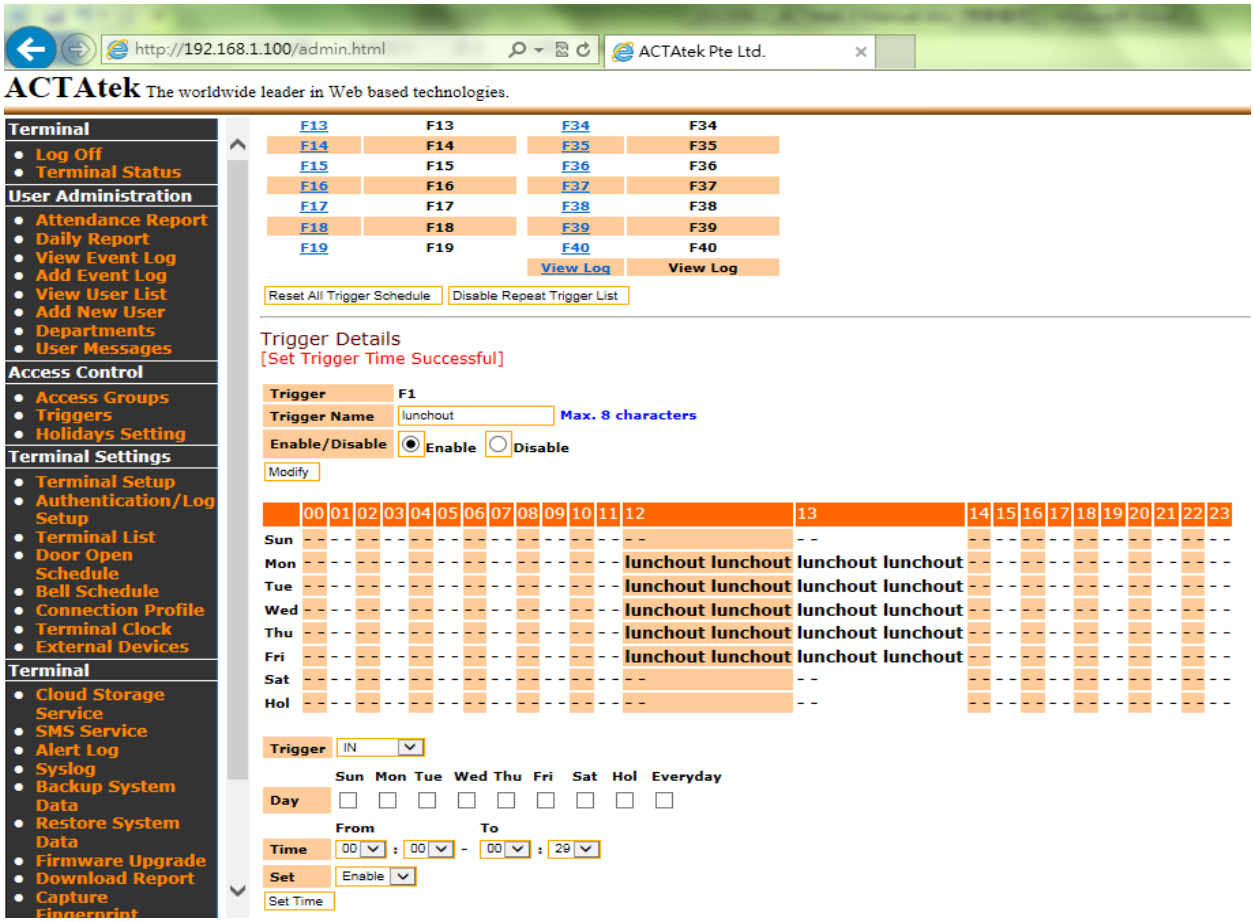
To view or modify the details for the relevant trigger, click the “Trigger” on the left of the Trigger Name.



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 ACTA4 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.



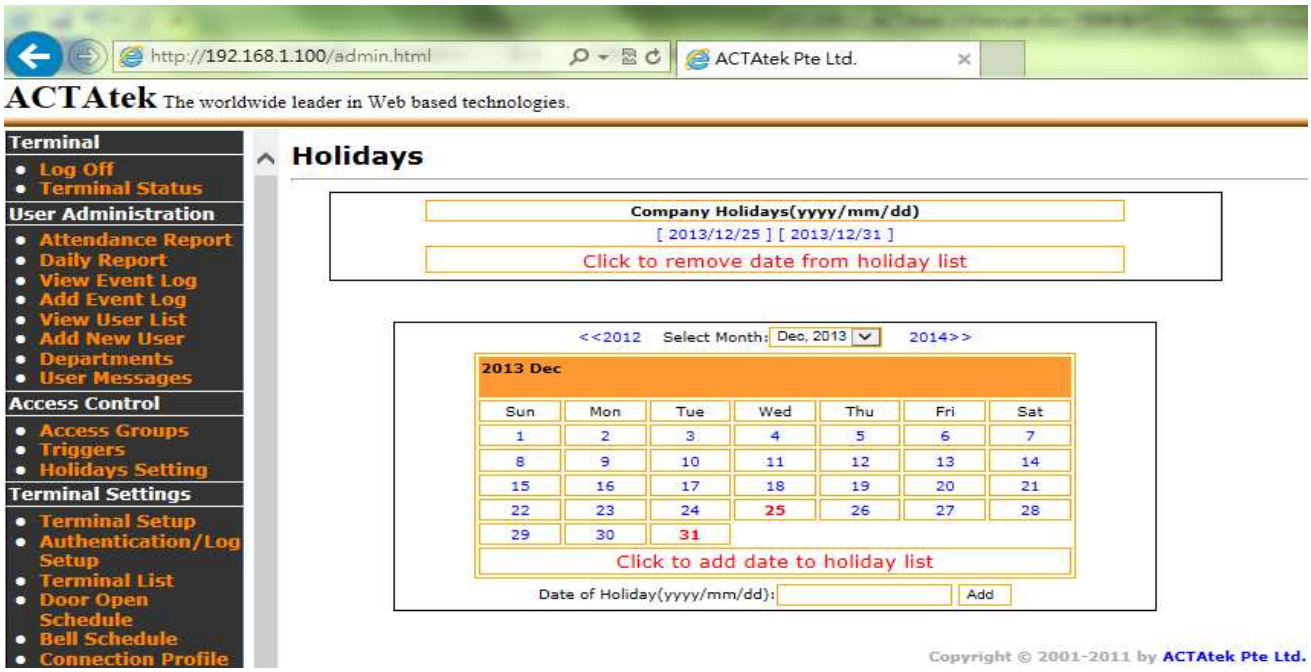
To modify the time settings & other information for the relevant trigger displayed, The information to be modified includes:

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:



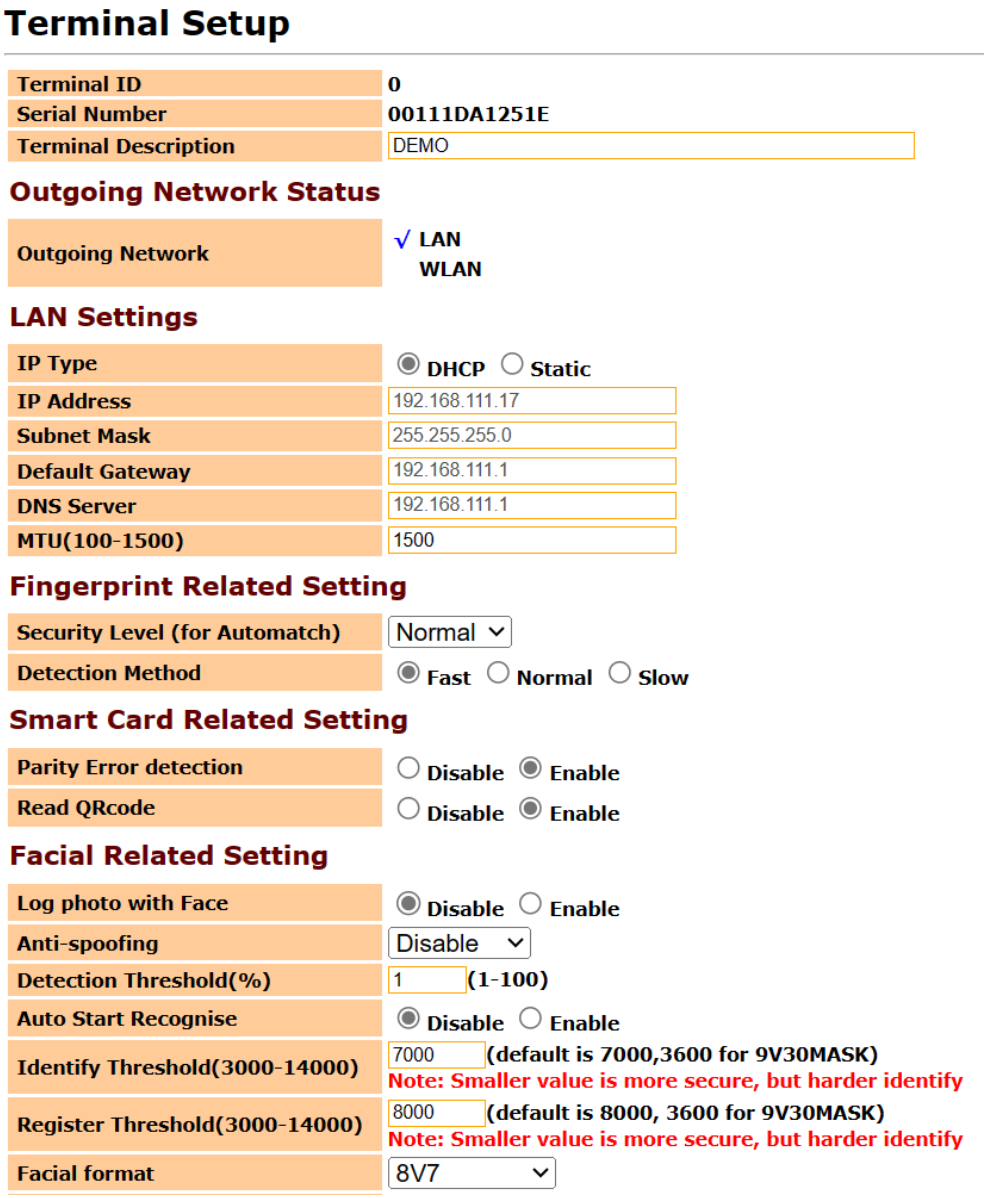
To add a new holiday, either click on the calendar to find the dates to add. Or type out the date in yyyy/mm/dd format and click "Add".

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.



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

Terminal Description	- The Description of the terminal
Outgoing Network	-The network connection of the device (LAN or WLAN)
IP Type / IP Address	- The IP Address of the terminal (DHCP 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.
MTU	- Please keep the default MTU setting(1500).
-)Fingerprint Related Setting:	
Security Level (for Automatch)	- The Fingerprint Security level for the device. Lower the level for higher and successful matching rate.
Detection Method &Threshold	- To change the FingerPrint detection setting ,and the threshold value will help to setup different sensitivity of the FP scanner under different installation environment.
-)Smart Card Related Setting:	
Parity Error detection	- To enable or disable parity error detection for HID prox. cards.
-)Facial Related Setting:	
Log photo with Face	-To enable or disable take User's Face photo
Anti-spoofing	-To enable or disable anti-spoof for Facial. **[Method2]**:for non-AT Facial model **[Method3]**:for AT Facial model
Auto Start Recognise	-To enable or disable auto-start Facial. ***If disable auto-start,User can press F4 key to start Facial.**
Detection Threshold	-The User's face size threshold to start facial recognition. e.g.The larger value will need a larger face.(stand close distance to the device)

Identify Threshold	-for normal user threshold when doing facial recognition.(default is 7000) Note: Smaller value is more secure, but harder identify
Register Threshold	-to identify the similar face when enrolling Face Users.(default is 8000) Note: Smaller value is more secure, but harder identify
Facial format	-**8V6***(old/existing installation) or **8V7****(new installation) or 9V30MASK(new installation)

*For the existing enrolled FACE Users,please change to **8V6**.

For new installation, please keep **8V7 as the default setting. It is using the new Facial algorithm with new facial template data for better facial identification/recognition.

Note:

Please take note that 8V6 and 8V7 are different Facial template data. So it will be required to re-enroll all FACE Users if upgrading to use new 8V7 for the existing/old 8V6 FACE users.

**For new installation,if needed,the new 9V30MASK supports Facial recognition with mask, and also mask detection. I

-)Console Display Timeout Settings:

Welcome Message Timeout	-You can select from 0.5 sec to 3 sec.
Console Display Timeout	-You can select from 30 sec to 1 hour.
Console Clock Format	-You can choose 12 hrs. or 24 hrs.
Idle Key light color	-You can change the idle keypad backlight color.
Door Bell Blinking	-You can disable/enable door bell button blinking
Touch Sensitivity	-You can adjust the keypad's Touch Sensitivity
Wiegand Configuration	- This option is to enable Wiegand output from the unit to the external I/O board or on-board Wiegand output data format.
Terminal Mode	-**Standalone**: the device will work with SOAP/API or master/client setup.

- **Access Manager**: the device is able to register with the Access Manager Suite.

Job Code	-Disable / Enable. **(See Appendix A.)**
Door SW Mode	-Choose Door Switch or Door Sense or Door Event OUT /IN
Door Sense 1&2 Option	-Choose Normal Close or Normal Open
Door Strike 1 Option	- Setting for Door Strike to open door.
-Emergency Mode	-For users who were assigned to EMERGENCY department can open door. **(See Appendix 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

*(*Door Strike2 is required to connect to external I/O board .)*

Language	- This option lets you select between various languages.
Webserver Port	- Specify other port to use for the webserver.
Web https Port	**-**Specify other port to use HTTPS 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.
Schedule reset	-To setup time for device check
Body Temperature Threshold	-When ACTAtek Temsen is installed,the default is 37.5.If the User's body temperature exceeds the threshold value setting,the device will reject the access .
User Consent Message	**-** To enable/disable user consent message for new Face / FingerPrint Users

8.4.2. Authentication/Log Setup

Authentication/Log Setup

Log Setup

Log Event	○ Disable ◉ Enable User Log
Log Size	1000 k
Log Unauthorized Event	○ Disable ◉ Enable
Accept Unregistered Smartcard	◉ Disable ○ Enable
Photo Option for Log	☑ Authorized Event ☐ Unauthorized Event
Web Add Record	○ Disable ◉ Enable
Accept Unregistered Facial	◉ Disable ○ Enable
Case open/close event log	○ Disable ◉ Enable

Authentication

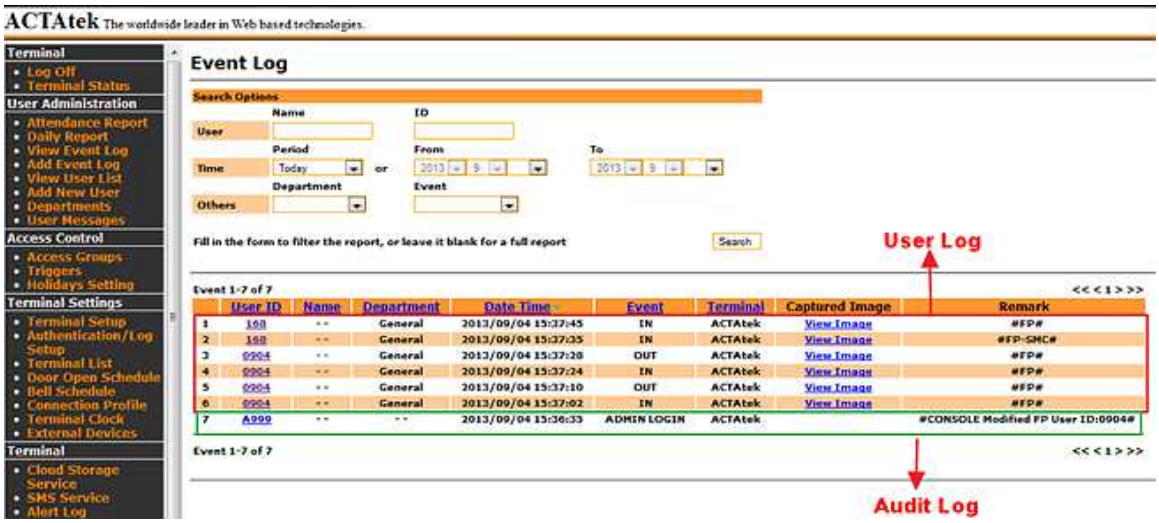
Additional Security Options	◉ Disable ○ Auto IN/OUT ☐ Auto Reset IN/OUT ☐ Reject Repeated Event in 5 sec(1 - 86400) ○ Anti-passback (Note: Anti-pass back will be reset at 00.00 hours) ○ Lunch Break Lock Out min (1 - 120) ○ Crowd Control Limit 1 (1 - 65535) Daily reset time 00:00 (hh:mm) Note: Additional login settings are now controlled from Access Manager
Fingerprint + Facial	◉ Disable ○ Enable
Gauth mode	Disable

Submit Reset

Log Setup

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

Note:To enable logs for 'User Log' or 'Audit Log' or both to be viewed from [View Event Log].See below.



-**Log Size:** To choose to store off-line event logs storage size.e.g.10K or 75K or 500K.

-**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.

- Web Add Record: To disable or enable add User time records from the device's webpage.

-Accept Unregistered Facial: To disable or enable to accept unregistered facial.(Guest mode)

-Case open/close event log: To disable or enable to log case open/close event log

-)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 23:59 hrs 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.

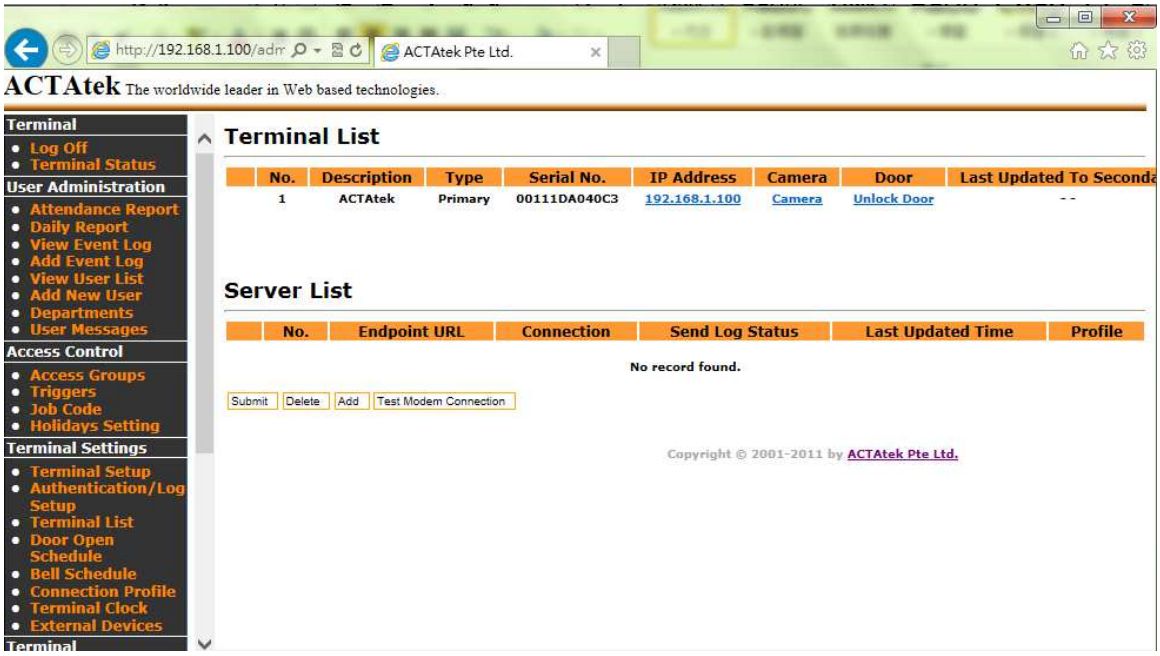
-Crowd Control Limit: The number of occupancy limits setting will be displayed at the device's LCD IN event ID e.g.IN(5), if there are 5 IN events already, the 6th IN event will be rejected as "Exceeded Occupancy Limit" until there is an OUT event . ***Standalone mode support.***

-Fingerprint + Facial: To disable or enable FP+Facial two-factor authentication.

-**Gauth mode:** To enable or disable Google authentication app. mode

8.4.3. *Terminal List*

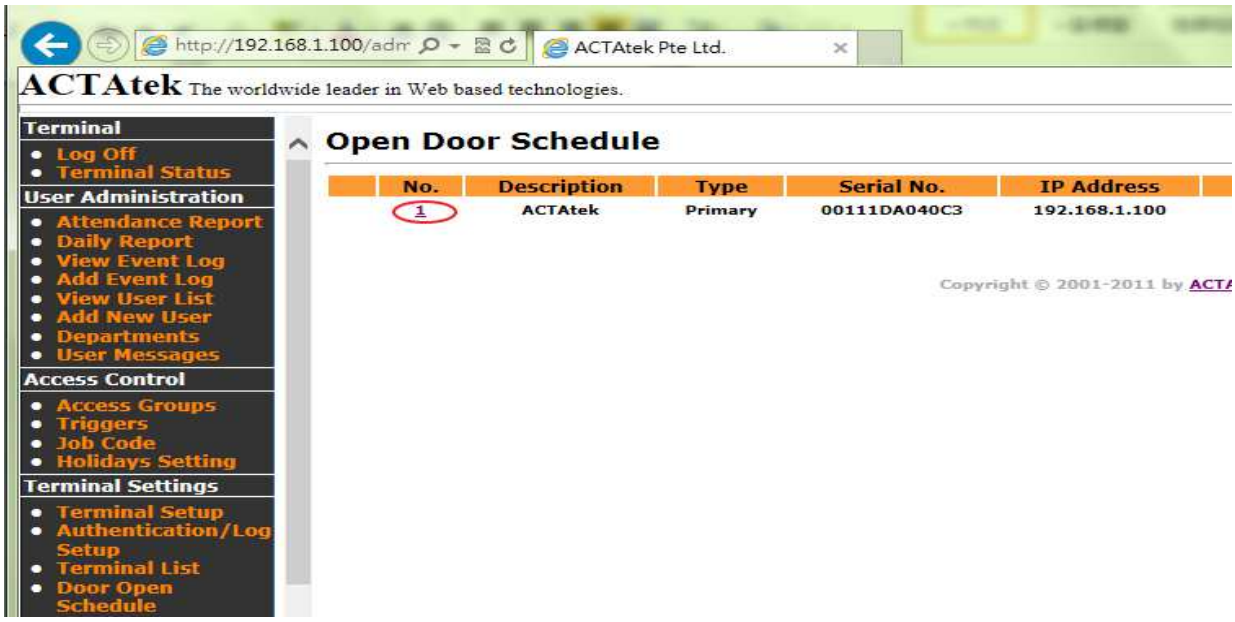
The “Terminal List” option under “Terminal Settings” can be used to view the list of terminals, and their respective name, type, serial number and IP Address, as shown below.

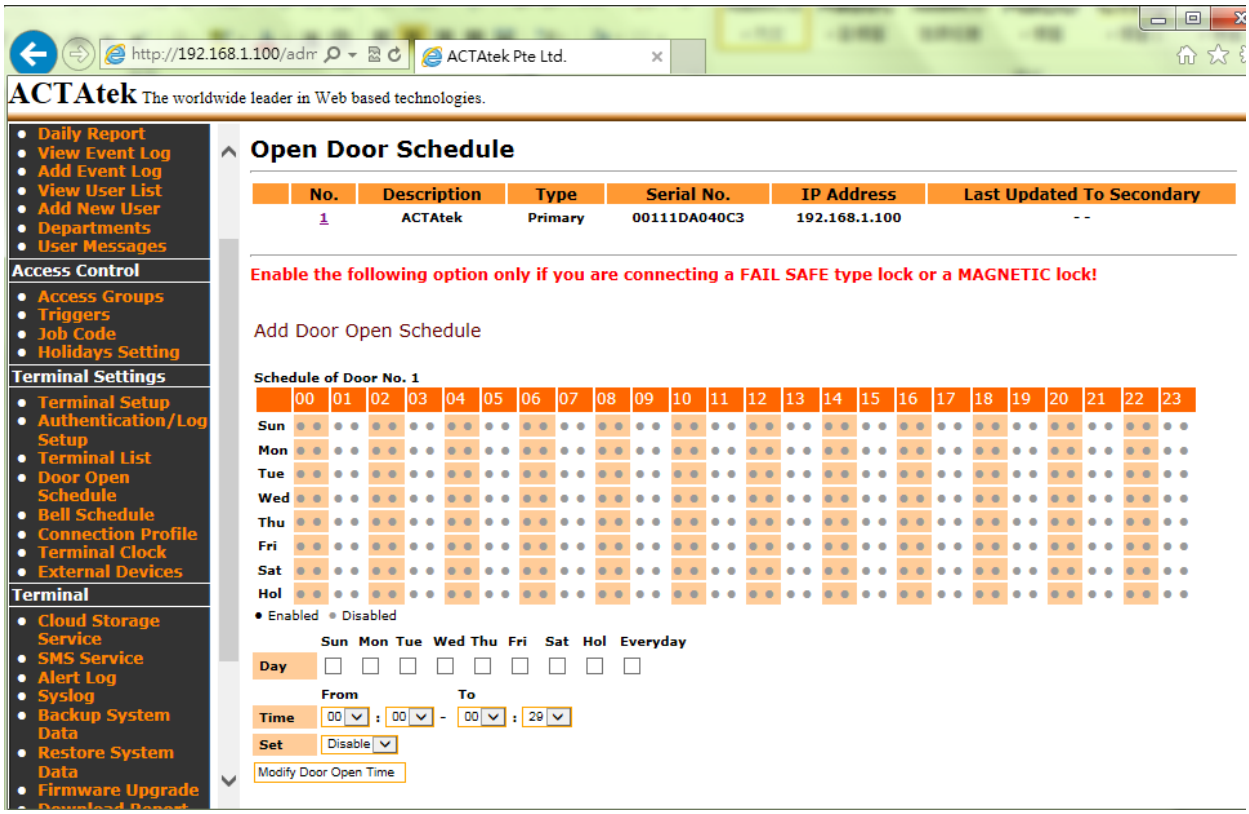


Under ‘Server list’, you can check the Event Logs sending status about the last sync. date and time with Agent ver.2’s or Access Manager Suite software’s back-end database.

8.4.4. Door Open Schedule

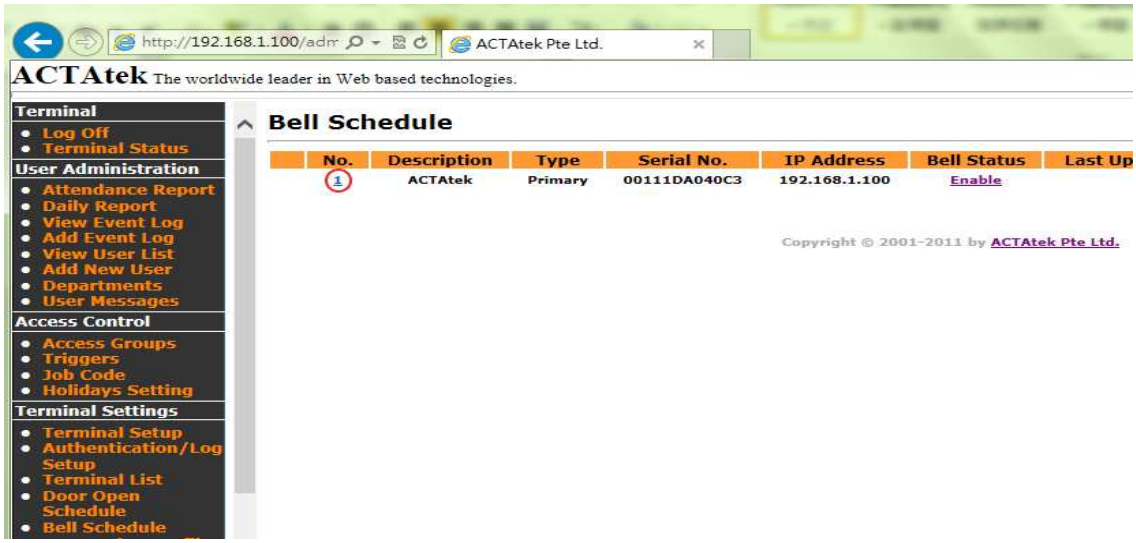
The Open Door Schedule is a feature to control the open access to the door entrance. Fill out the parameters in the page to set up the time for the open access time of the door entrance.

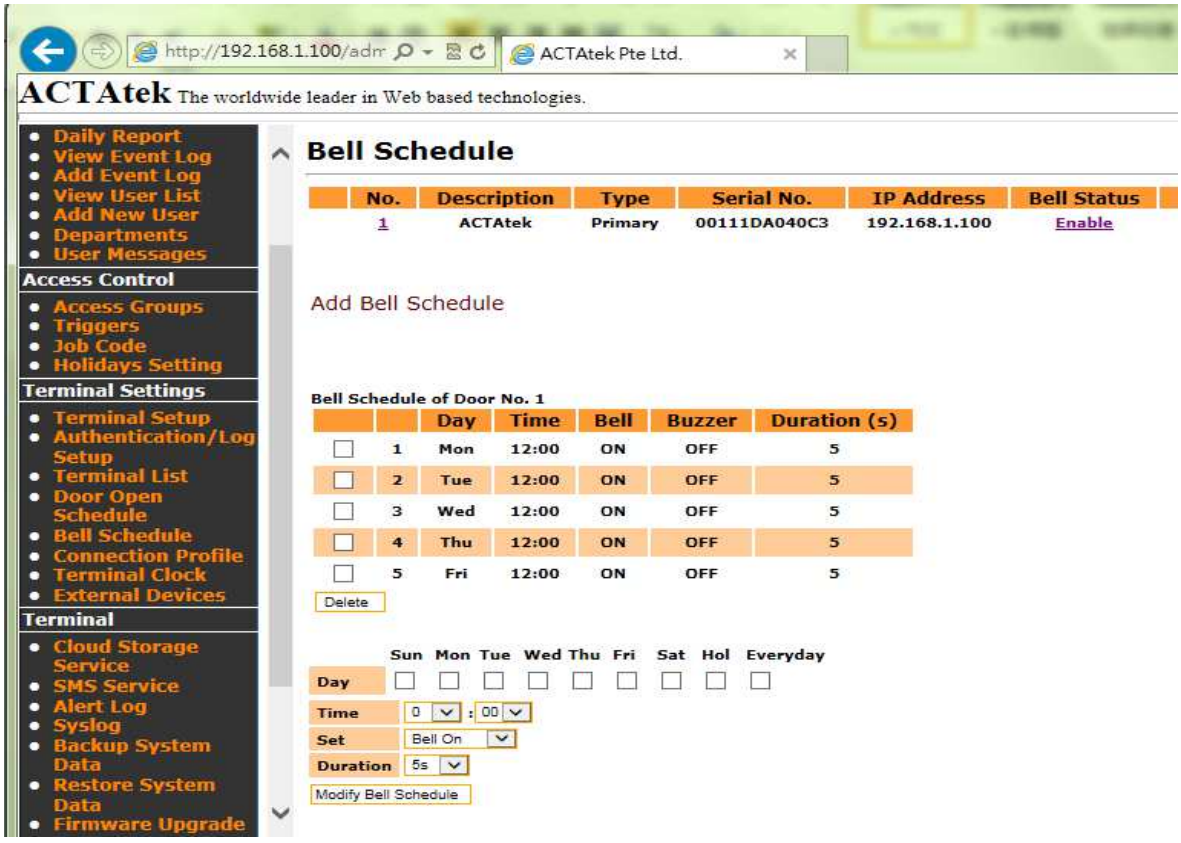




8.4.5. Bell Schedule

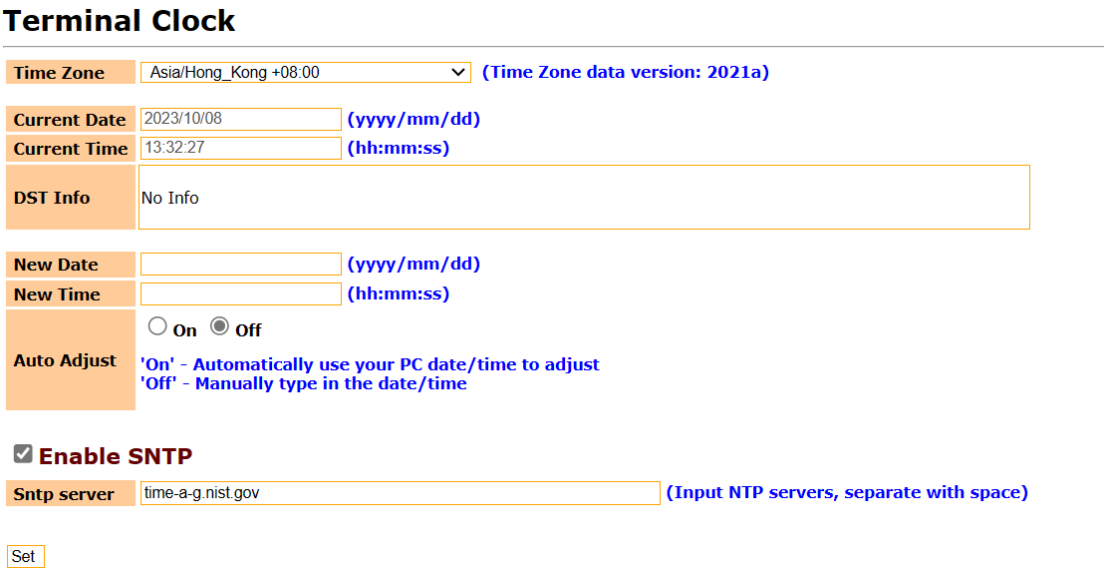
The Bell Schedule option needs to be enabled via Door Strike 2 Option under Terminal Setup page. Once enabled, ACTA4 is able to trigger a bell wired to the door strike 2 connector for the scheduled time.





8.4.6. *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.



If the SNTP (Time server) is enabled, then the ACTA4™ will sync. its time with SNTP server each 3 hours.

Note: 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 ACTA4™ 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.

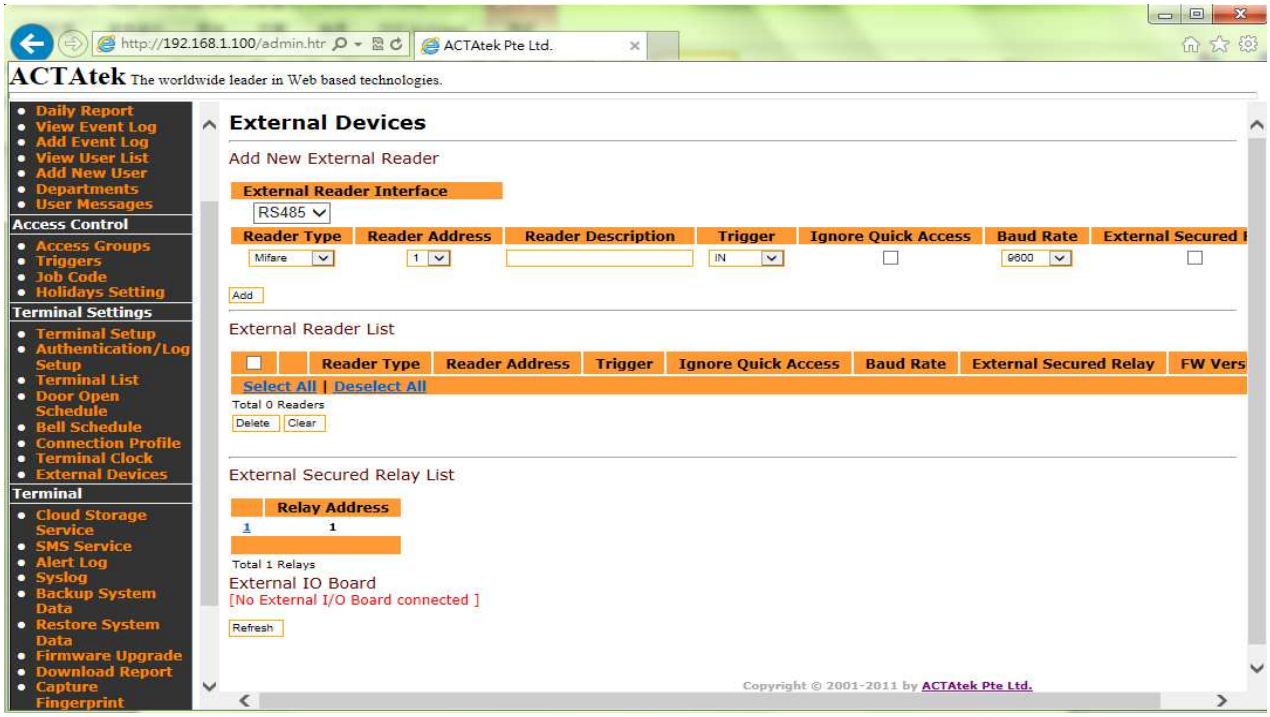
To let ACTA4™ to follow the time on the PC, select “On” for Auto Adjust. To disable this auto adjust, select “Off” and the time setting will be available for users to input the “New Date” and “New Time”. Click ‘Set Time’ to set the device’s date/time after “Auto Adjust” finished.

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

Click “Set” to save any modifications made.

8.4.7. External Devices

If ACTA4 was connected to the external I/O board, you can see the connection status at external devices page.(Note: The device will automatically detect the external I/O board once powered on and connected.)



8.4.8. DDNS

First, please sign up a DDNS account e.g. http://www.noip.com/

After that,you will have the below Login detail to be entered into the device's DDNS page. And then click [Submit] button. The device will run the DDNS client to update its current public IP address to link with the Host Name that you had applied .Once it is done, you can access to device's webpage via the signed up DDNS name.

For example:

User name/Email: actatek.sg

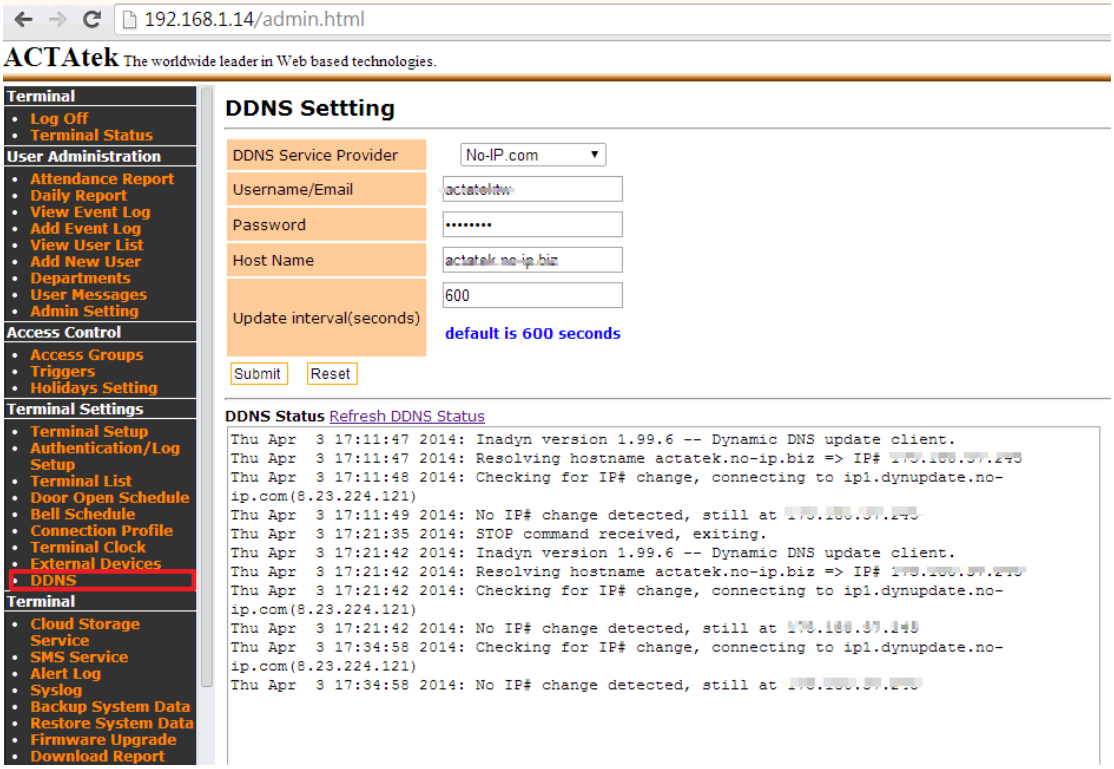
Password:actatek

Host name:actatek.no-ip.biz

Note:Please make sure below.

-The device's IP setting is able to access the Internet.

-If the device was using private IP address (LAN),it will be required to setup the port-forwarding at the router setting. See the http://setuprouter.com/ about how to configure it.



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

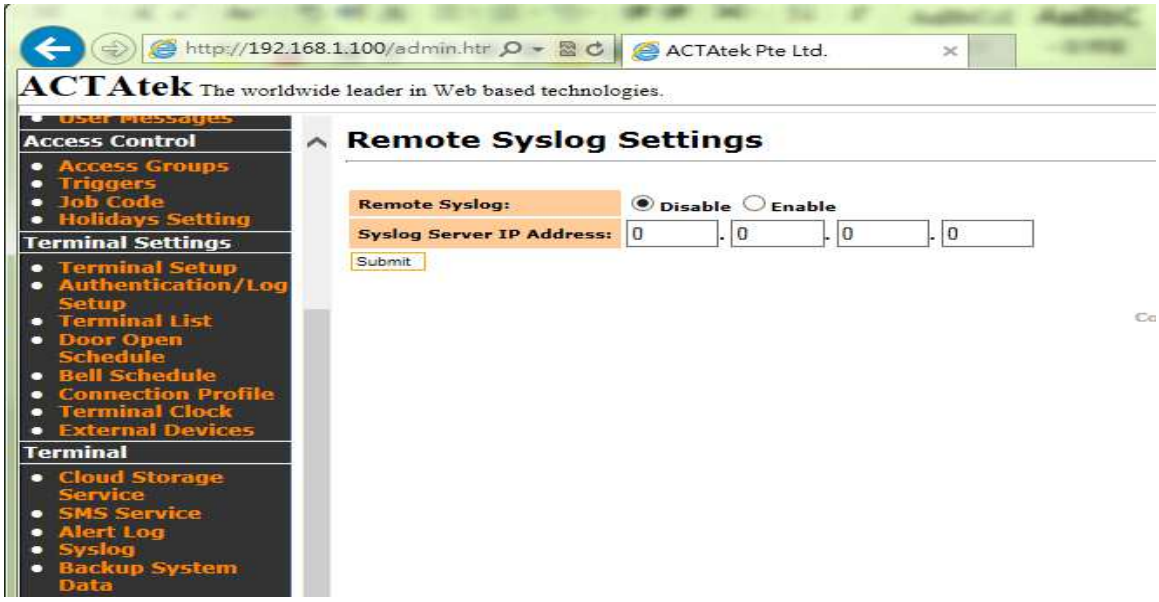
Administrator's Email Address	
SMTP Server Address	
SMTP Port	0
SMTP Security	STARTTLS
SMTP User Name	Note:please leave it blank if not use user authentication.
SMTP Password	Note: Please leave it blank if you don't want to change/add the password.
SMTP TEST	Send Test Email
Administrator's SMS No	

NO.	Type	Email	SMS
1	Door is opened more than 30S	☐	☐
2	Bottom case is detached	☐	☐
3	Primary is offline	☐	☐
4	Duress access	☐	☐

Save Reset

8.4.12. Syslog

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



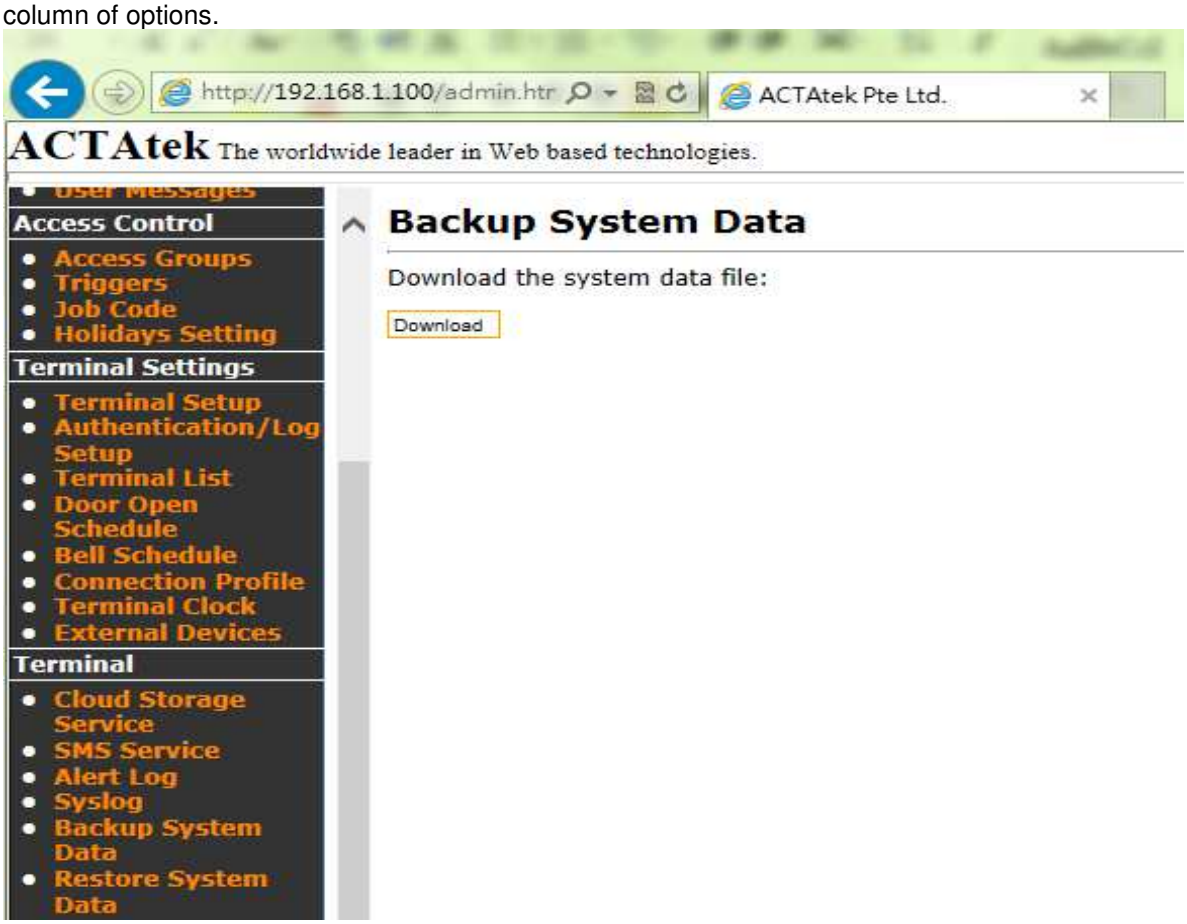
8.4.13. Backup System Data

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.

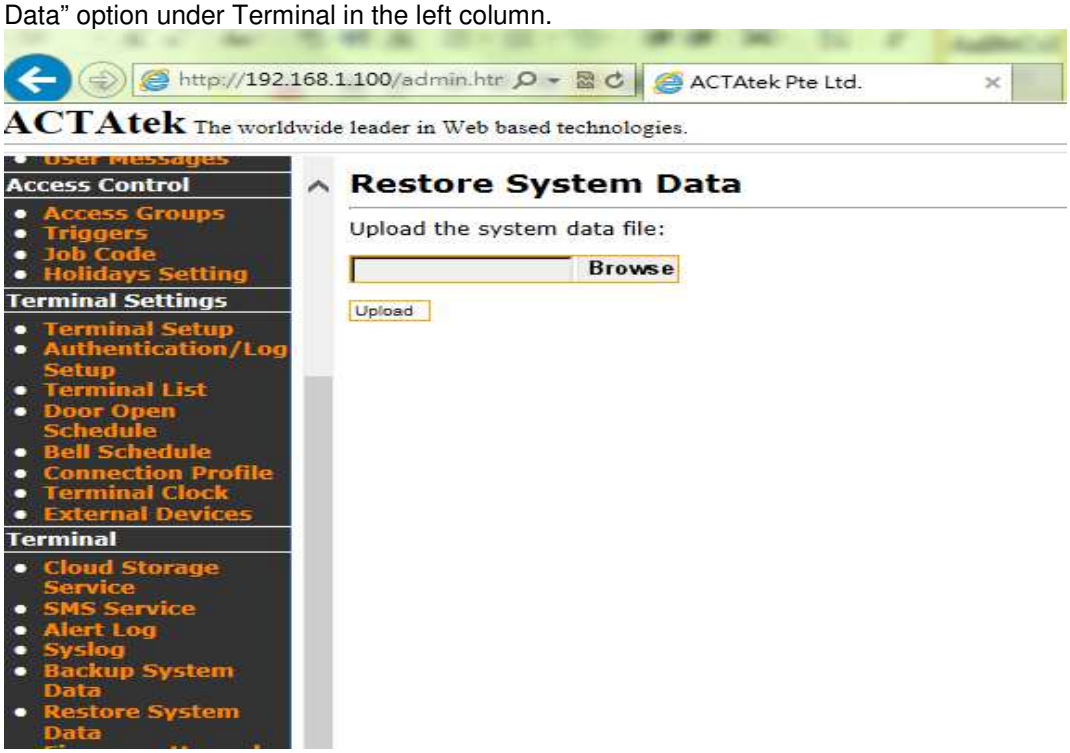
To backup the system configuration, click on “Backup System Data” under Tools from the left column of options.



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.



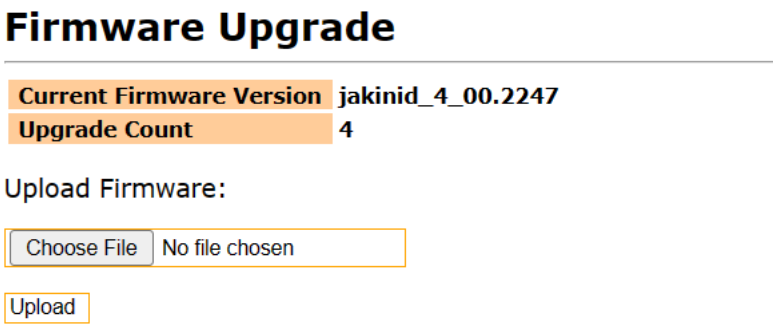
Click “Browse” to locate the specified and previous backup system file, once located, click “Open”.

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

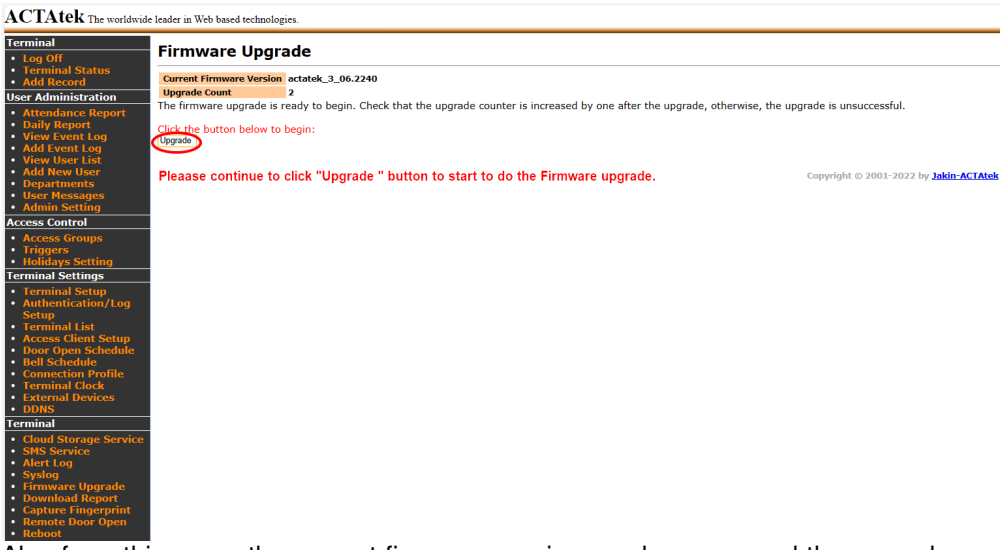
8.4.15. Firmware Upgrade

Firmware releases will be carried out on a regular basis. ACTAtek R&D team will continue to add new features to ACTA4, 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.

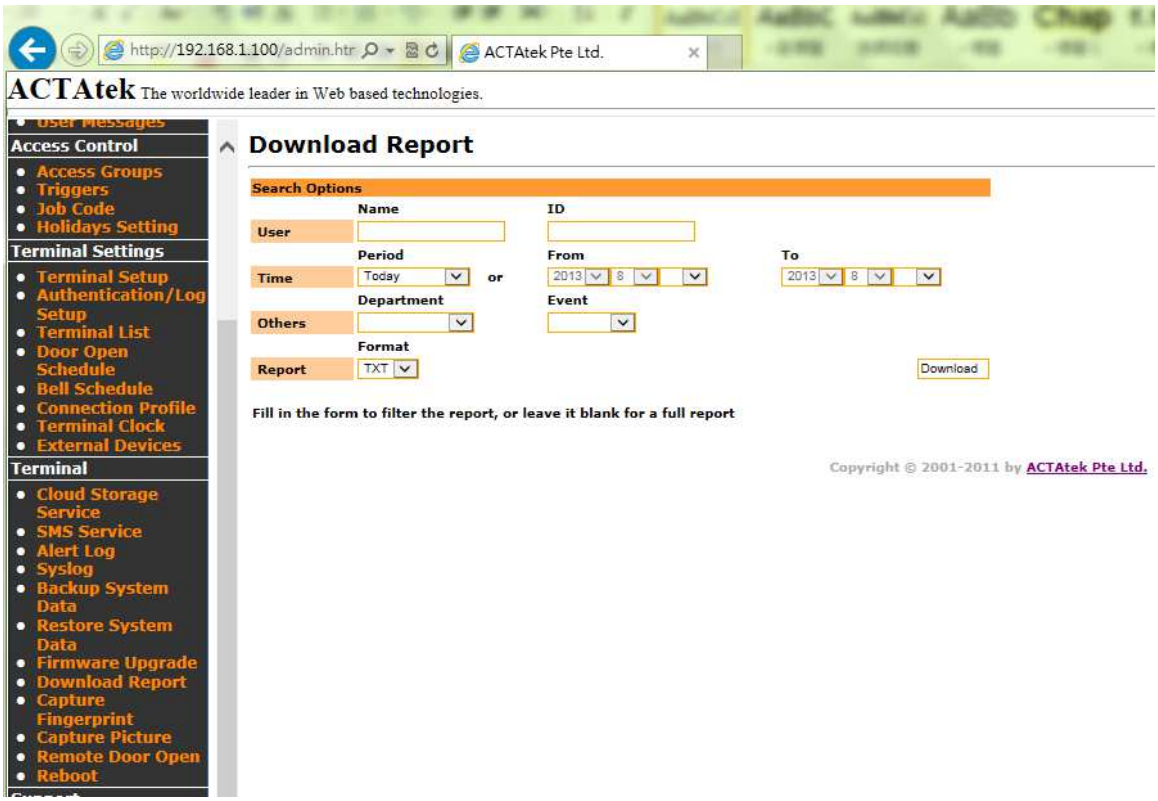


Also from this page, the current firmware version can be seen, and the upgrade count is also available to show you how many times the system has been upgraded, for your reference purposes. Once upload is clicked, the system will install the new firmware and your system will reboot automatically to let 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.



Reports can either be downloaded by:

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

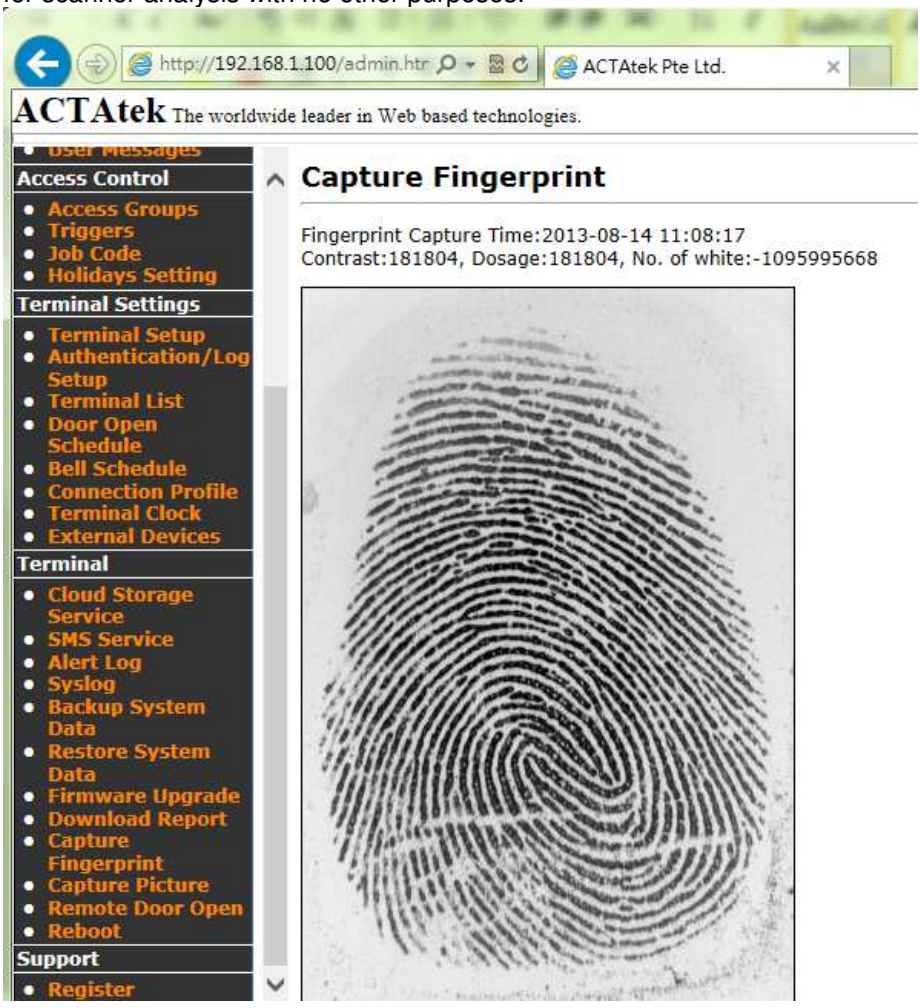
Click “Download” for the report to be downloaded to your system for payroll or other management purposes.

8.4.17. Capture Fingerprint

The ACTA4™ 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.

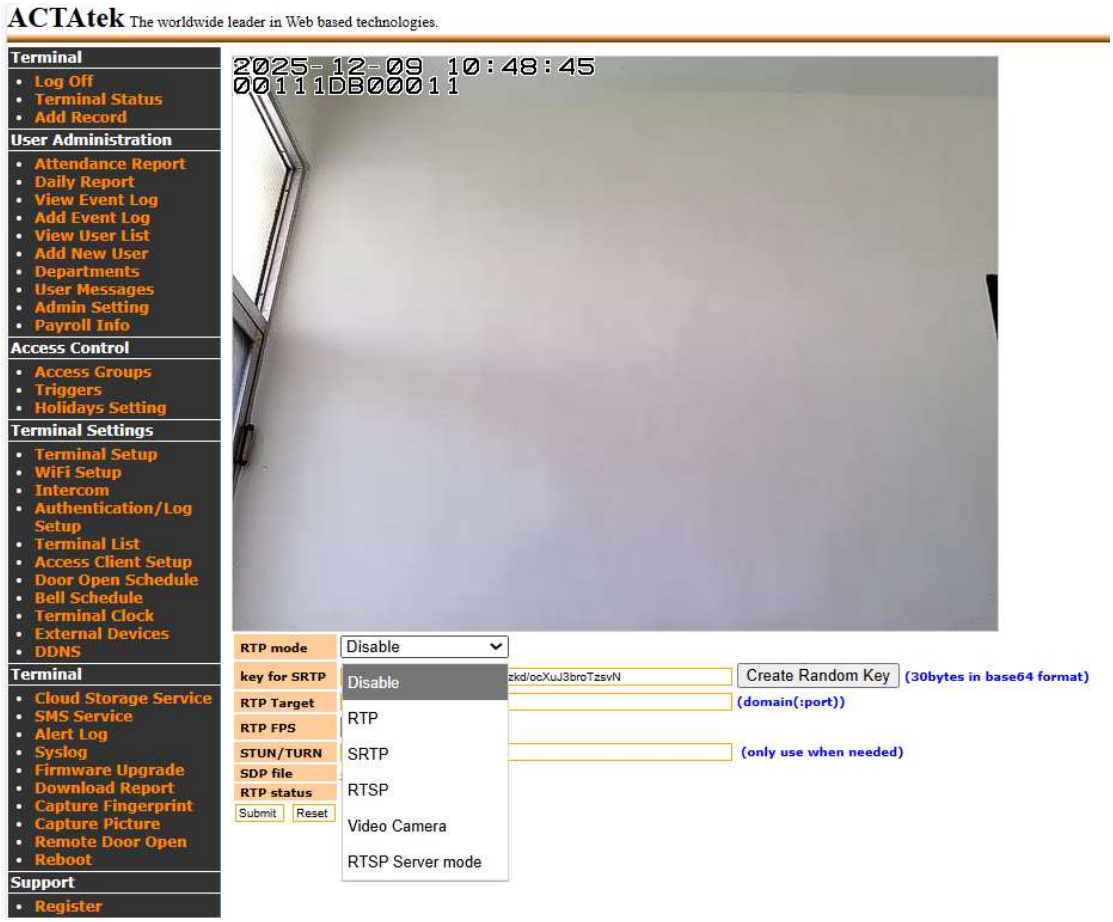
This image is captured via the terminal menu under “User Management” --> “Capture Fingerprint”. Once the fingerprint is captured, it can be viewed via the web interface, as shown below.

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 remote door open with live view or steaming the video to the VMS via RTSP mode.



RTP mode options:

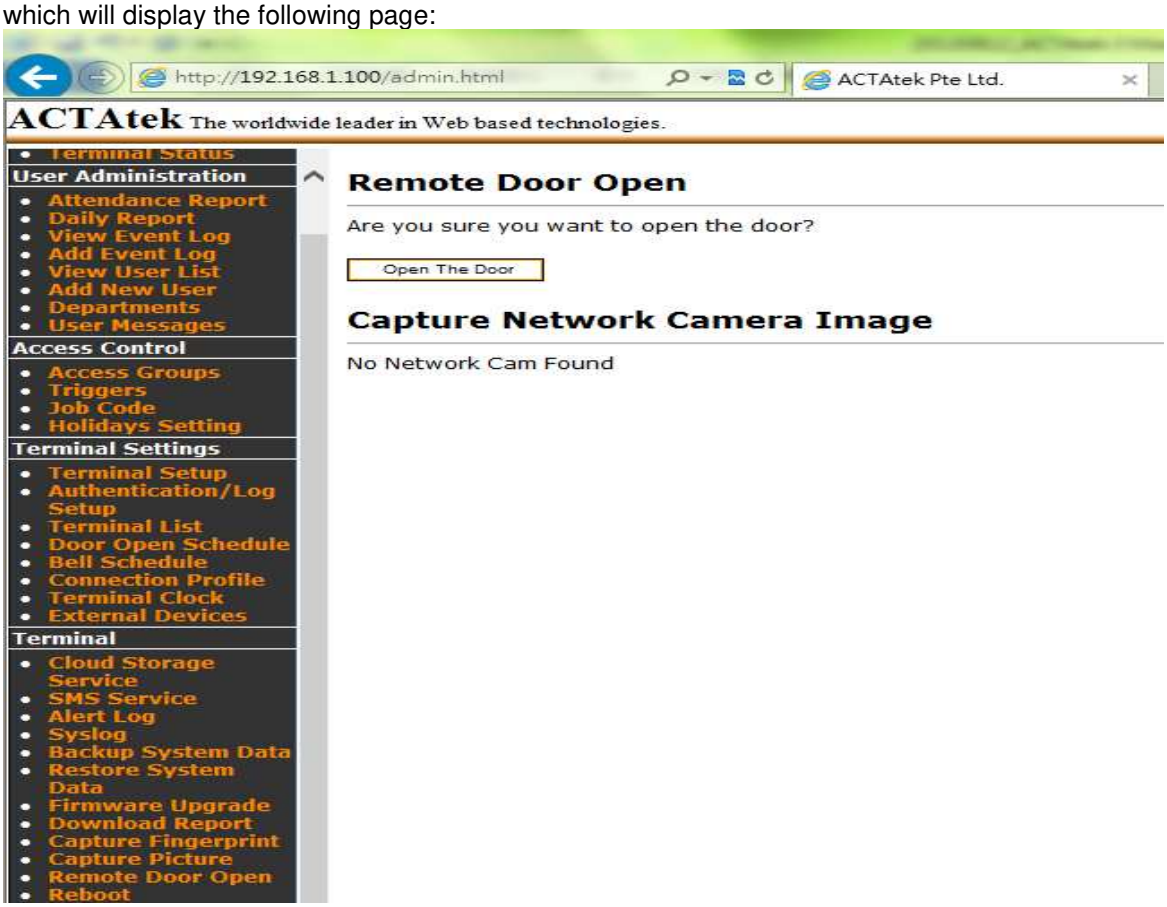
- **RTSP Push Mode** Streams video to an external RTSP server (e.g., MediaMTX).
  Example: rtsp://192.168.1.111:8554/stream
- **Video Camera Mode** View live video directly from the device settings page.
- **RTSP Server Mode** Device acts as an RTSP server; access via VLC or other clients.
  Example: rtsp://192.168.1.108:8554/cam

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.

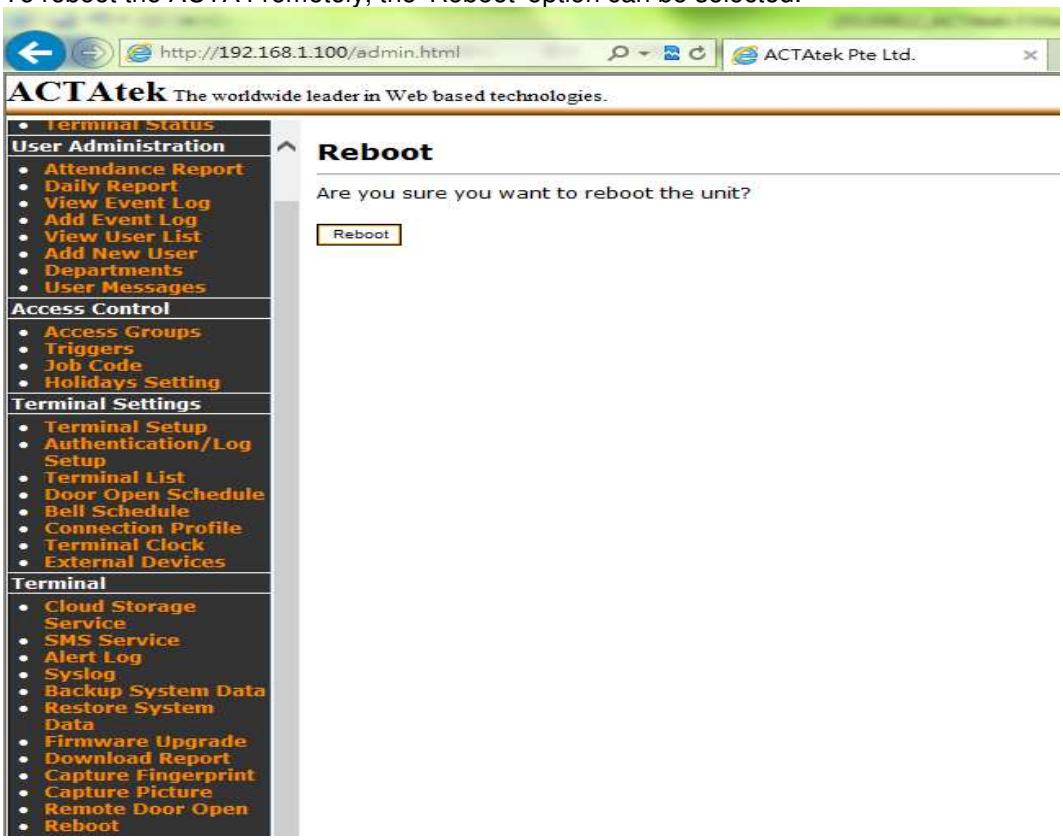
To open the door remotely from any computer, click on "Remote Door Open" under Tools, which will display the following page:



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 ACTA4 remotely, the 'Reboot' option can be selected.



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

8.4.21. Register

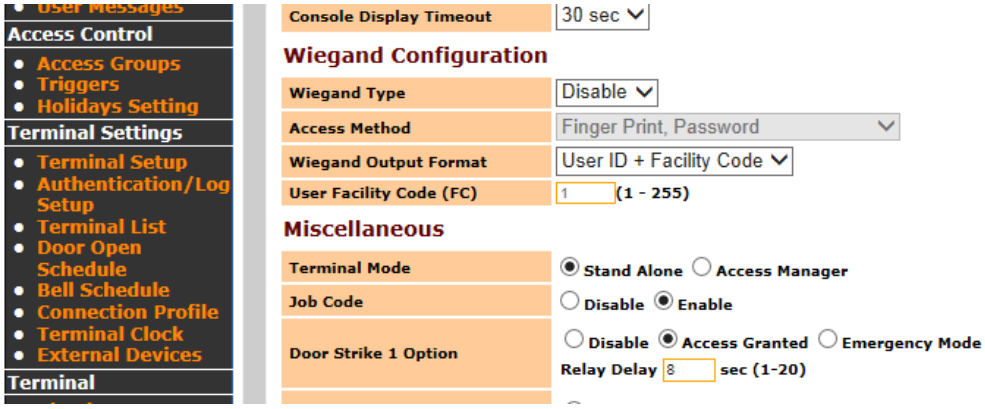
You will be redirected to our support website to register the device's warranty at our support website. Please follow up the product registration steps as shown in the webpage.

Appendix A. Job code feature

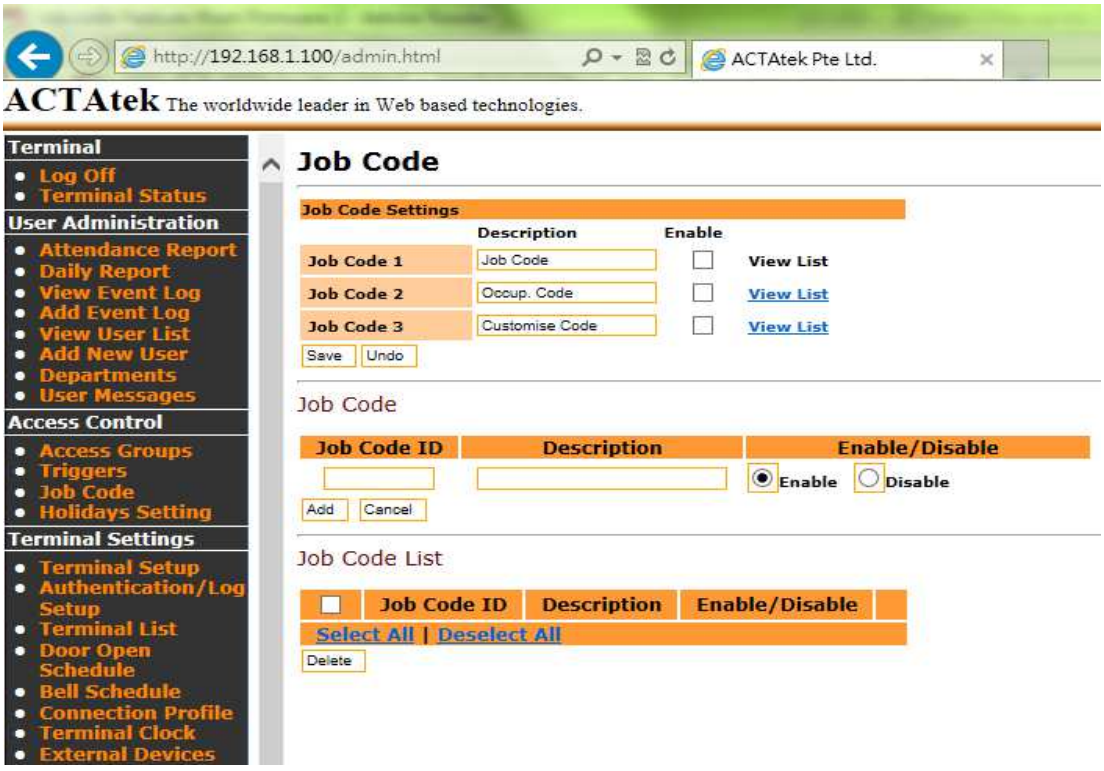
Job code is a new feature which allows ACTAtek to provide better capability to integrate with any third party payroll/HR programs. It is an advance idea that is extended from our existing trigger features. As before, the trigger feature from ACTAtek only supports up to 40 different descriptions of Event 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.



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



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.

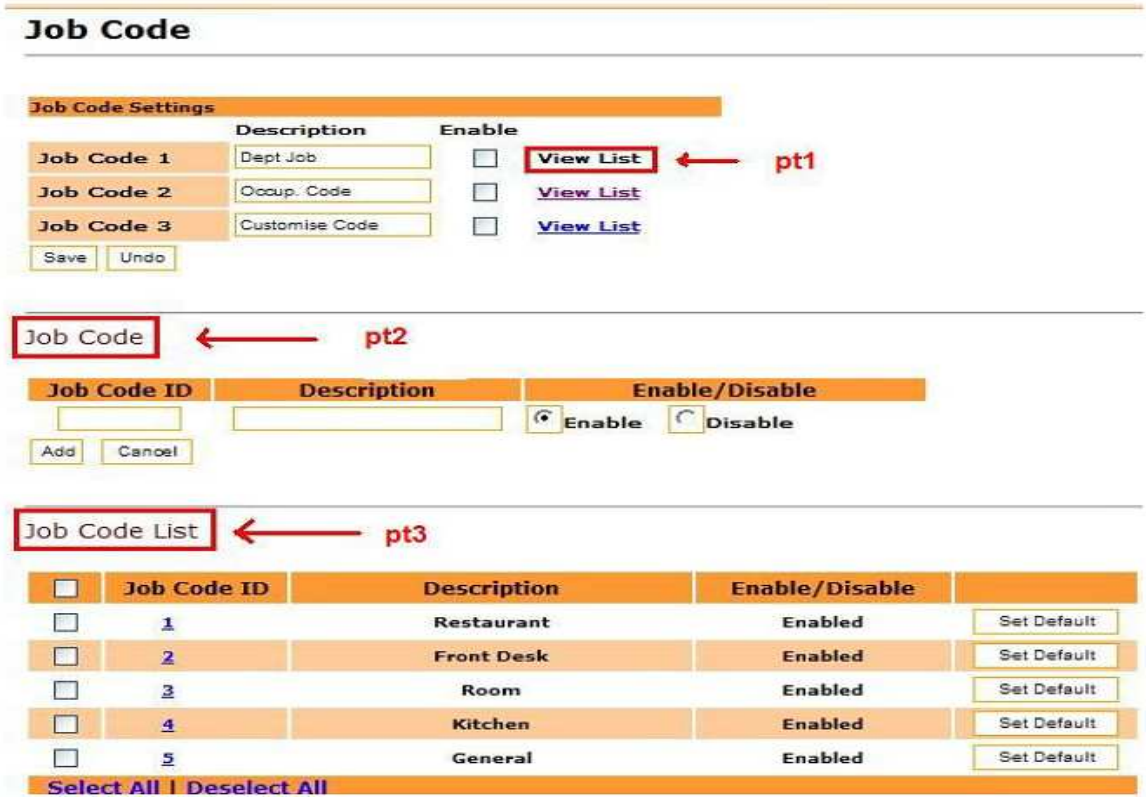
For each Job Code table, you could assign it with different descriptions.
For instance, in Job code 1, you may put "Job Department", in Job code 2, you may put "Occupations", and etc.

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 button 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).



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 of 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 3rd party controller connected to ACTAtek external I/O board. The 3rd 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 3rd 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 (3rd party controller) as shown on figure 1.

2. Actatek device will send wiegand userid data thought 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.

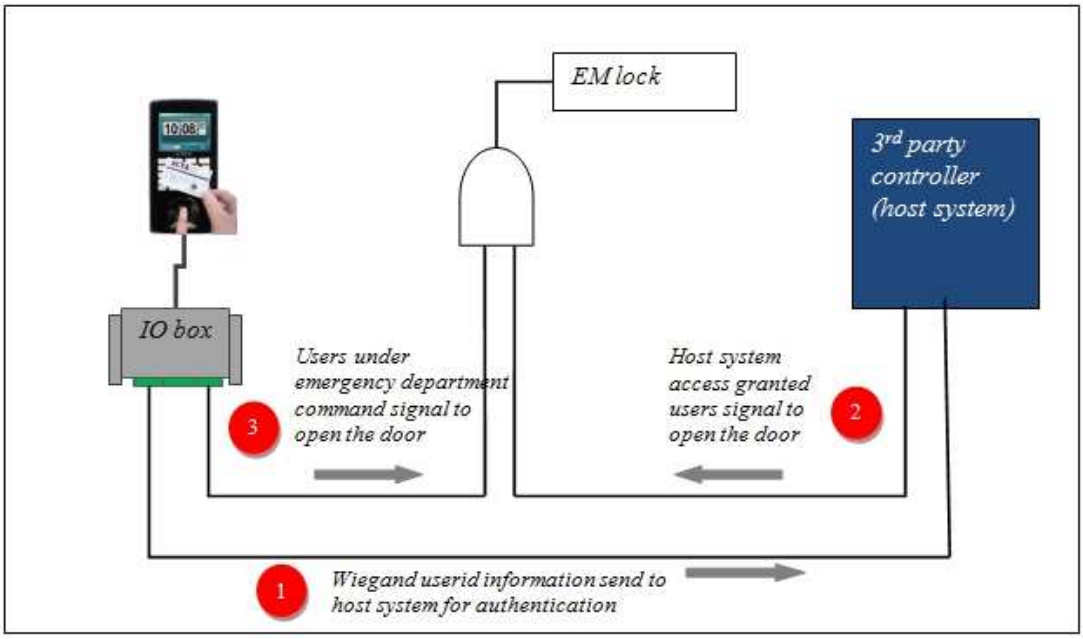


Figure1.Emergency mode

Alert Log Settings

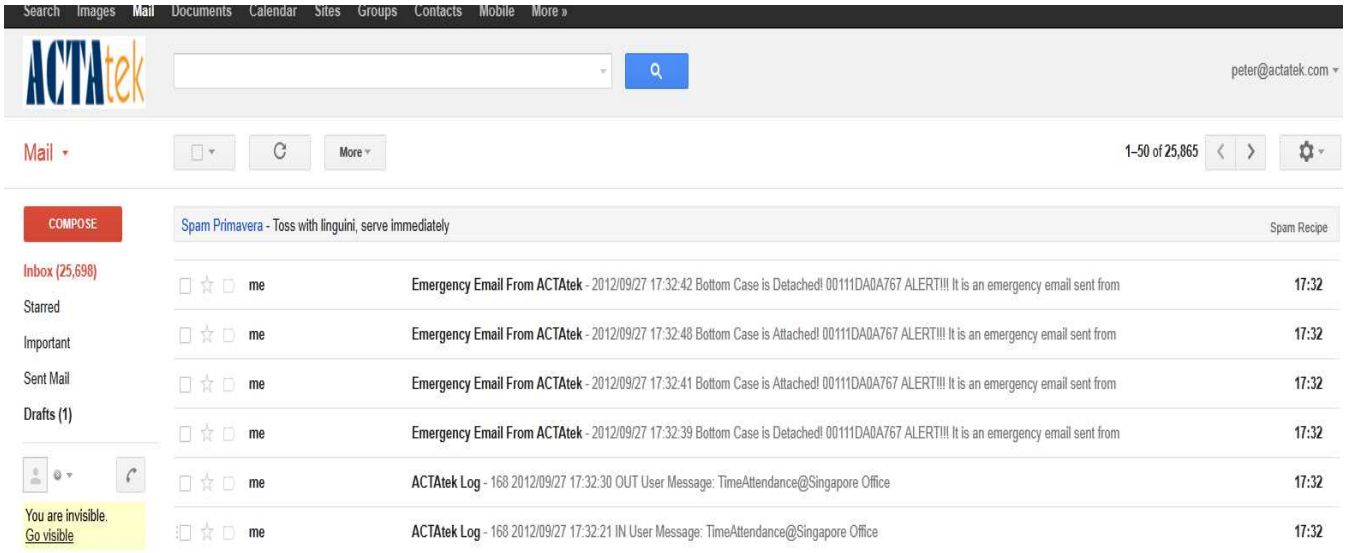
Administrator's Email Address	
SMTP Server Address	
SMTP Port	0
SMTP Security	STARTTLS
SMTP User Name	Note:please leave it blank if not use user authentication.
SMTP Password	Note: Please leave it blank if you don't want to change/add the password.
SMTP TEST	Send Test Email
Administrator's SMS No	

NO.	Type	Email	SMS
1	Door is opened more than 30S	☐	☐
2	Bottom case is detached	☐	☐
3	Primary is offline	☐	☐
4	Duress access	☐	☐

Save Reset

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

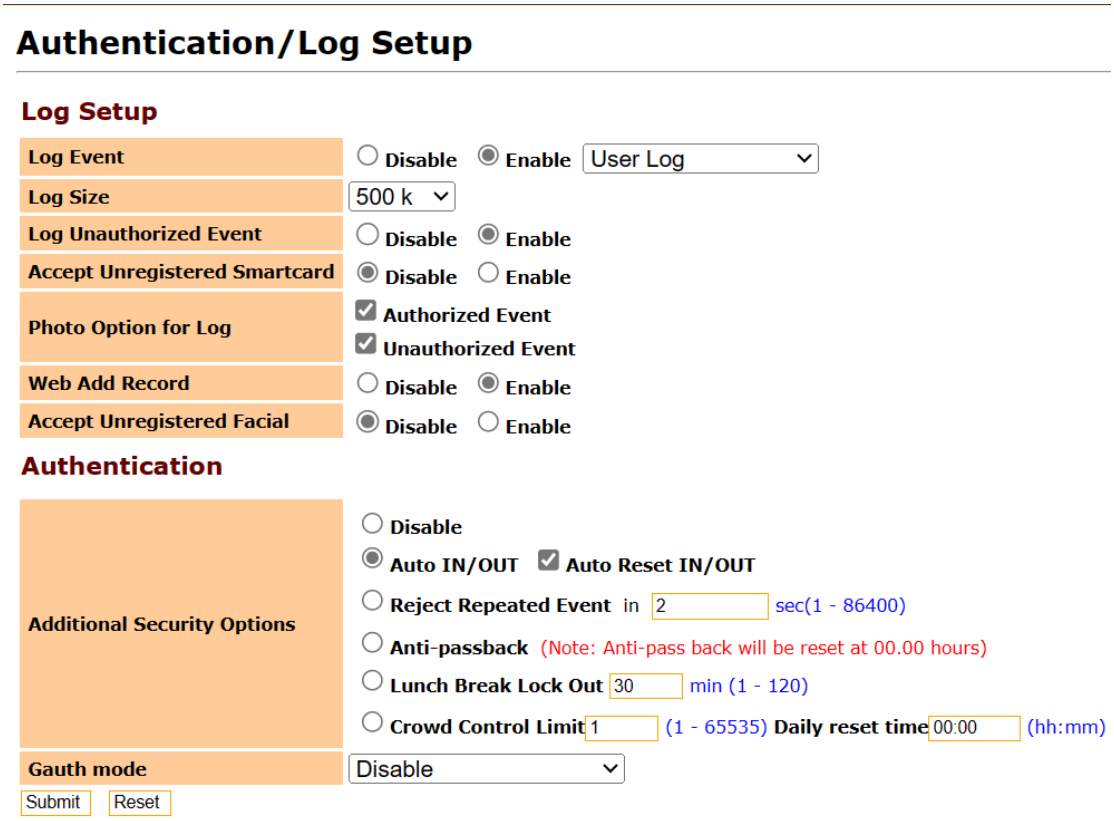
Note: If you did not receive the emails, please kindly check your [Spam] folder of the email account.



Appendix C. Additional Security Options

Auto IN/OUT:

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



- 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	7588	- -	2012/03/16	Friday	10:21:06 19:00:12	8.65

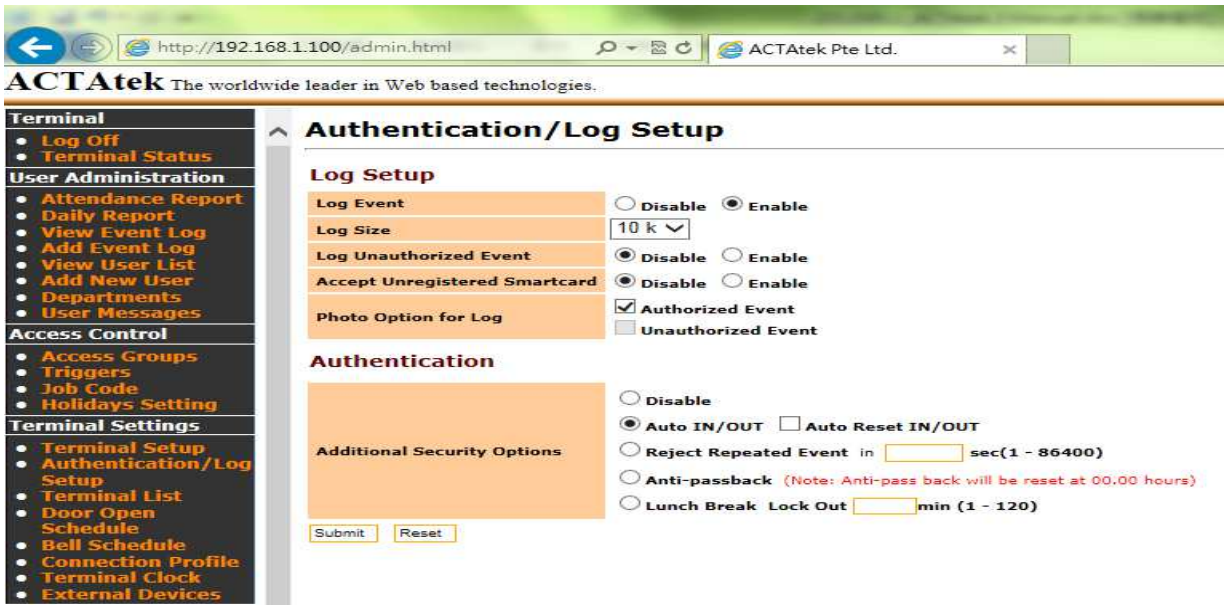
Reports 1 of 1 << < 1 > >>

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

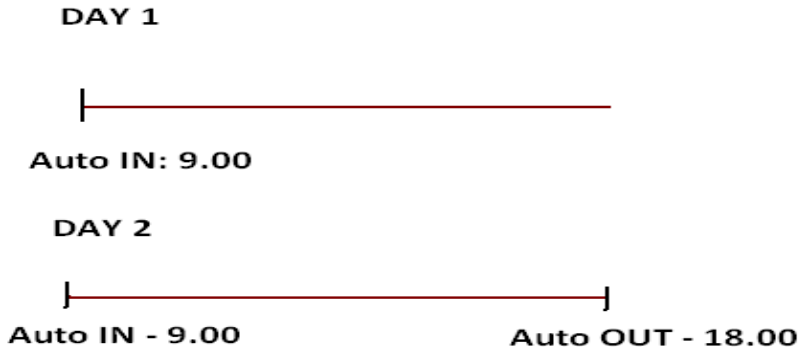
	User ID	Name	Department	Date Time	Event	Terminal	Remark
1	7588	- -	General	2012/03/16 19:00:12	OUT	ACTAtek	#SMC(SN:74DDF1EE)#
2	7588	- -	General	2012/03/16 10:21:06	IN	ACTAtek	#SMC(SN:74DDF1EE)#

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

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



Consider the following case:



- 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 > >>

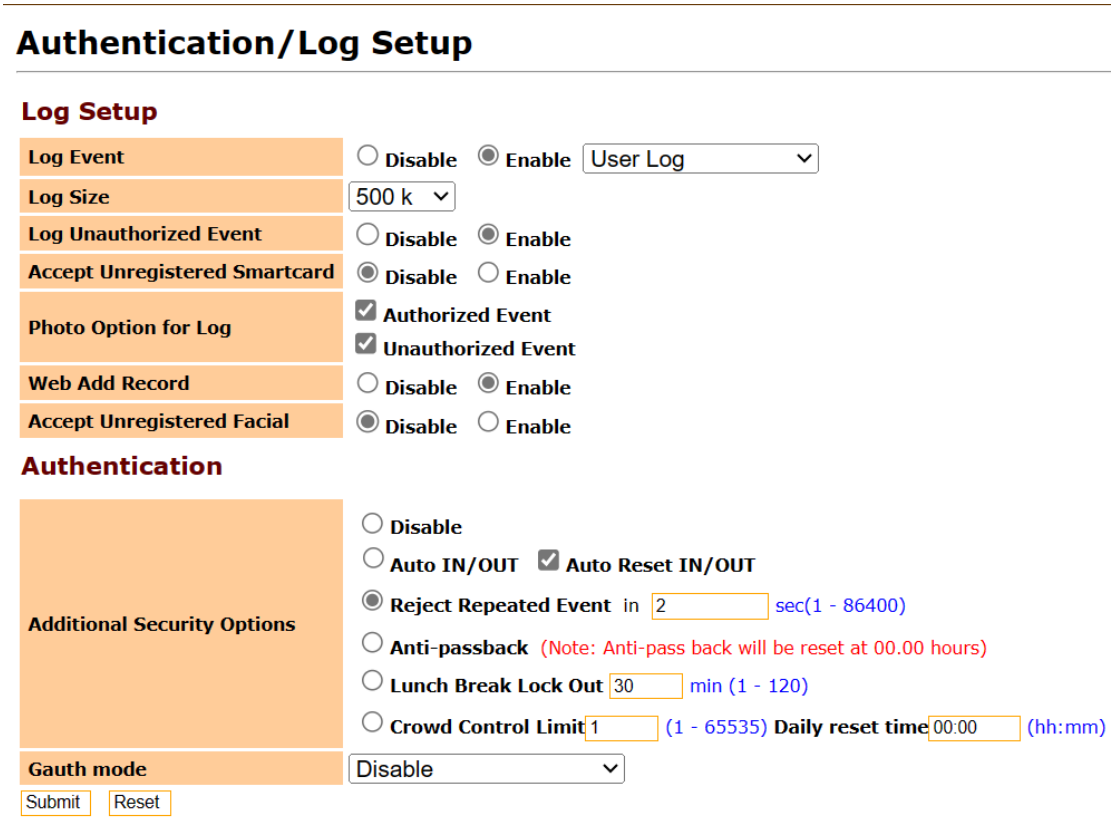
Event 1-3 of 3 << < 1 > >>

	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)#

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

Reject Repeated Event:

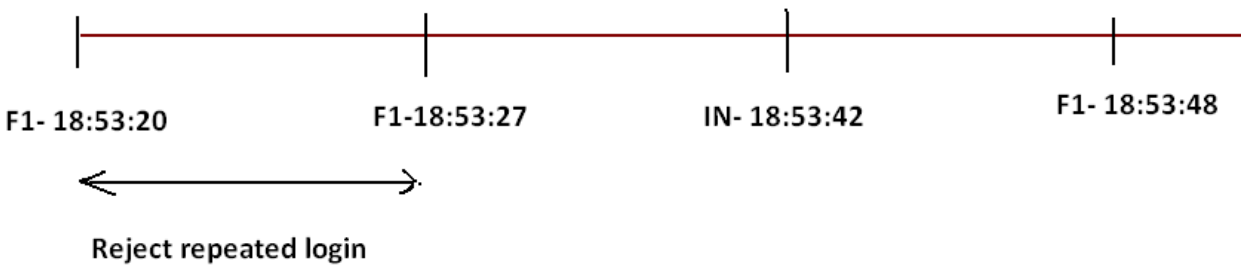
- Admin user can enable this feature at 'Authentication/LogSetup' web page.



- 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.

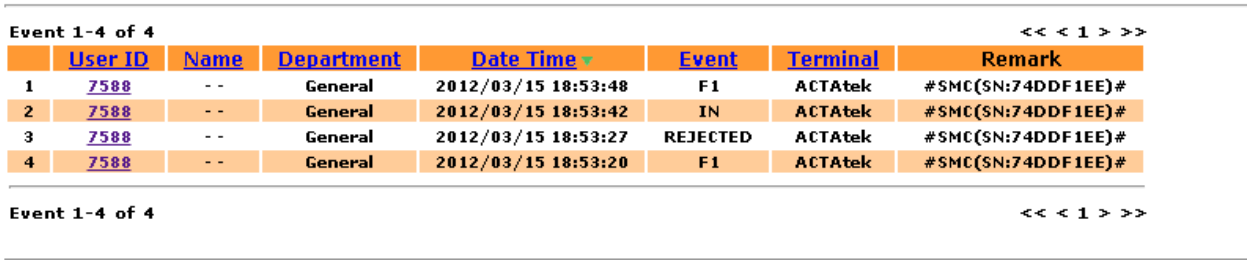
- Consider the following situation:



  - 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.



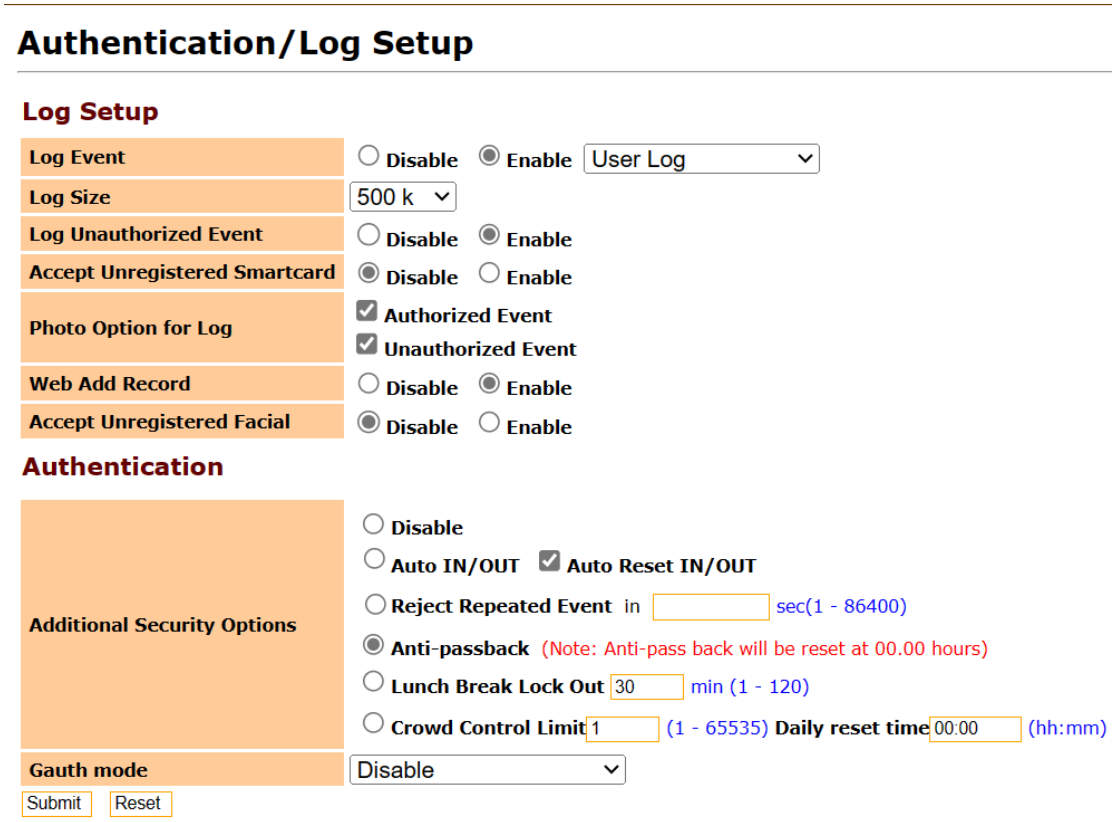
Event 1-4 of 4 << < 1 > >>

	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:

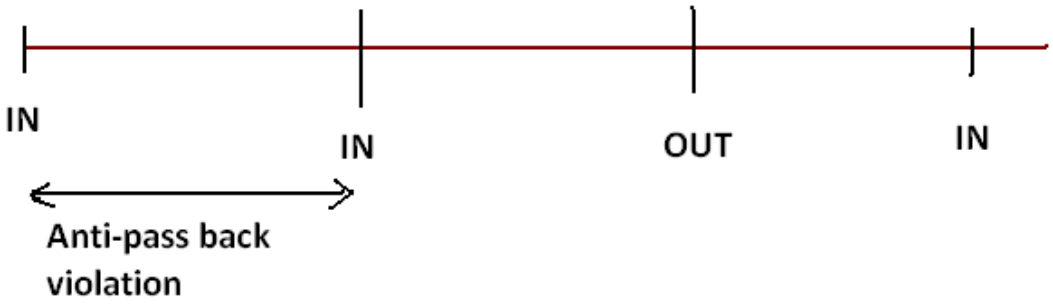
The main purpose of anti- pass back system is to prevent a card holder from passing their card back to a second person to gain entry into the same controlled area. This also improves the accuracy of roll call 'Last Known position' reports and deters tailgating. Anti- pass back sequence being 'IN-OUT-IN-OUT-IN-OUT'. 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.



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.

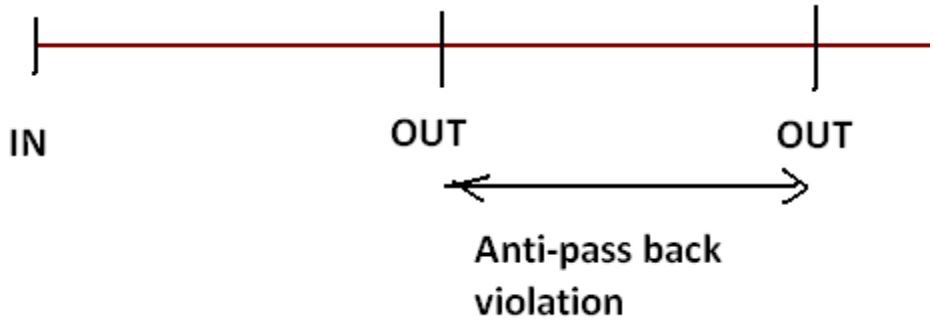
Following is the screen shot of event logs being generated:

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

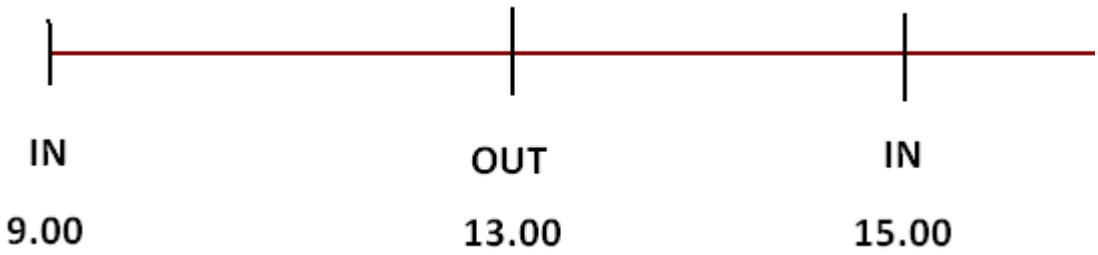
	User ID	Name	Department	Date Time	Event	Terminal	Remark
1	7588	- -	General	2012/03/15 18:33:28	IN	ACTAtek	#SMC(SN:74DDF1EE)#
2	7588	- -	General	2012/03/15 18:33:23	OUT	ACTAtek	#SMC(SN:74DDF1EE)#
3	7588	- -	General	2012/03/15 18:33:06	REJECTED	ACTAtek	#SMC(SN:74DDF1EE)#
4	7588	- -	General	2012/03/15 18:33:01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

Authentication/Log Setup

Log Setup

Log Event	○ Disable ◉ Enable User Log
Log Size	500 k
Log Unauthorized Event	○ Disable ◉ Enable
Accept Unregistered Smartcard	◉ Disable ○ Enable
Photo Option for Log	☑ Authorized Event ☑ Unauthorized Event
Web Add Record	○ Disable ◉ Enable
Accept Unregistered Facial	◉ Disable ○ Enable

Authentication

Additional Security Options	○ 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 30 min (1 - 120) ○ Crowd Control Limit 1 (1 - 65535) Daily reset time 00:00 (hh:mm)
Gauth mode	Disable

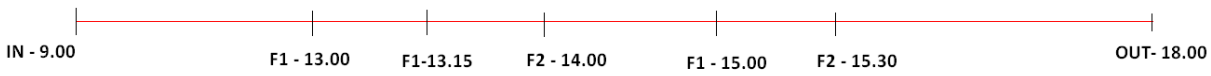
Submit Reset

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**

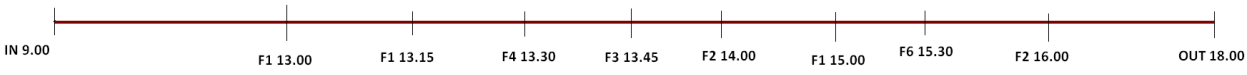
Total working hours **(working hour - (lunch 1 + lunch 2))**
(9 - (1 + 0.5)) = 7.5

Event 1-9 of 9 << < 1 > >>

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

Event 1-9 of 9 << < 1 > >>

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 << < 1 > >>

	User ID	Name	Date	Weekday	In Out	In Out	LunchIn LunchOut	LunchIn LunchOut	Total Working Hours
1	7588	- -	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 << < 1 > >>

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**

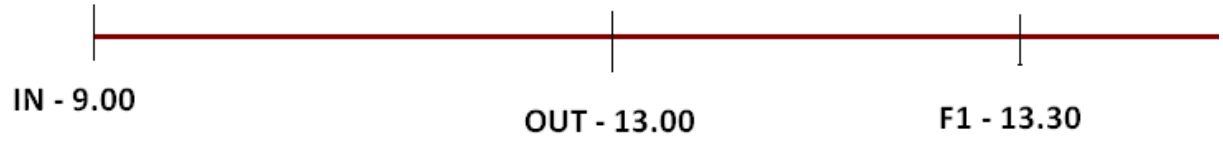
Total Working hour **(Working hour - (Lunch 1 + Lunch 2))**
(9 - (1 + 1)) = 7 hours

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**

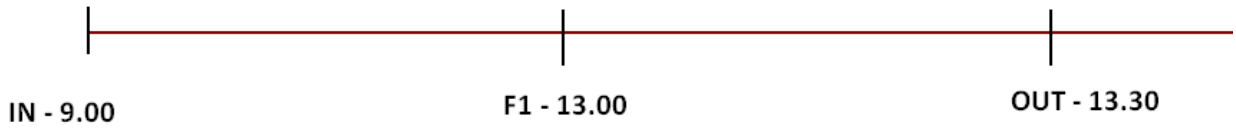
Total working hours: **4 hours**

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	7588	- -	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 > >>

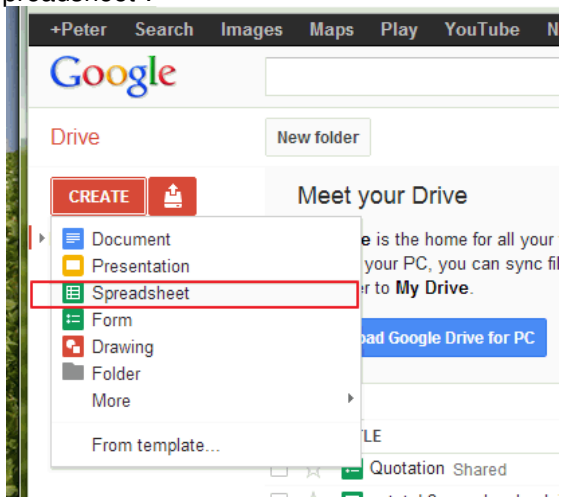
	User ID	Name	Department	Date Time	Event	Terminal	Remark
1	7588	- -	General	2012/03/15 13:30:10	OUT	ACTAtek	#SMC(SN:74DDF1EE)#
2	7588	- -	General	2012/03/15 13:00:14	F1	ACTAtek	#SMC(SN:74DDF1EE)#
3	7588	- -	General	2012/03/15 09:00:11	IN	ACTAtek	#SMC(SN:74DDF1EE)#

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

Appendix D. Cloud Storage Service

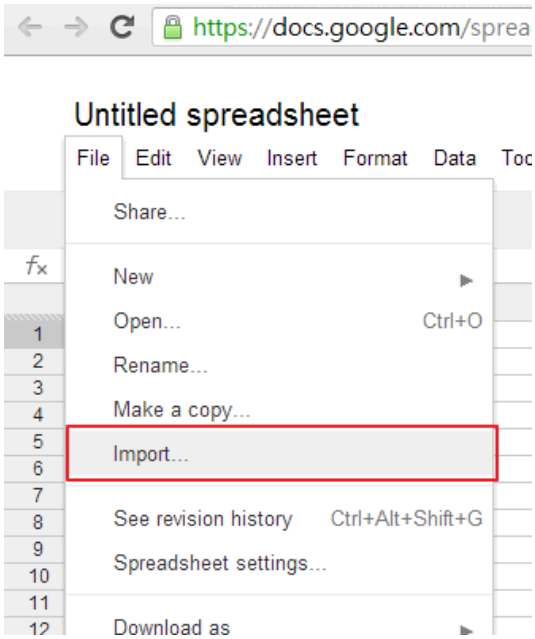
Step1. Login to your personal or company's Google Drive account.
https://drive.google.com/

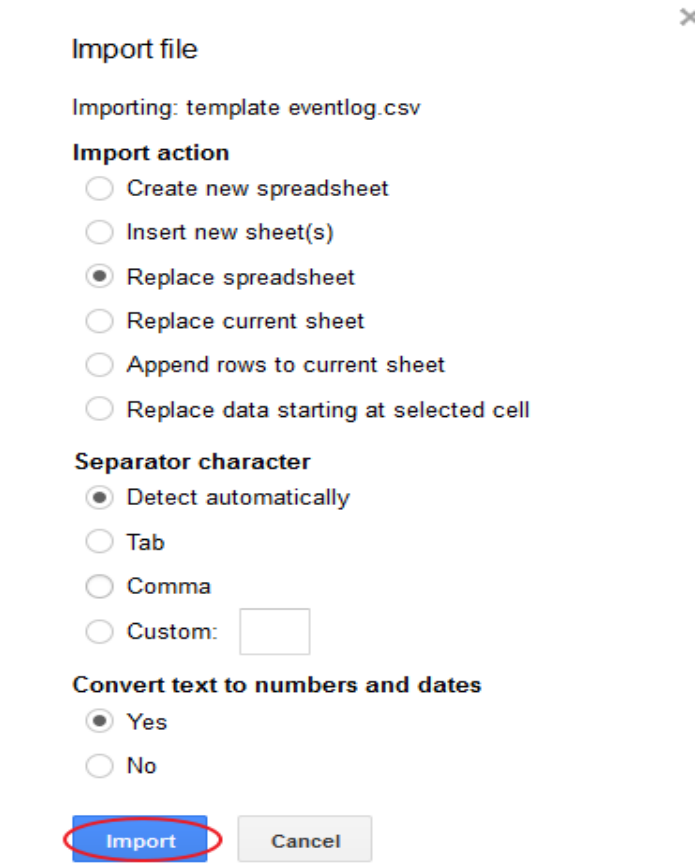
Step2. Create a "new spreadsheet".



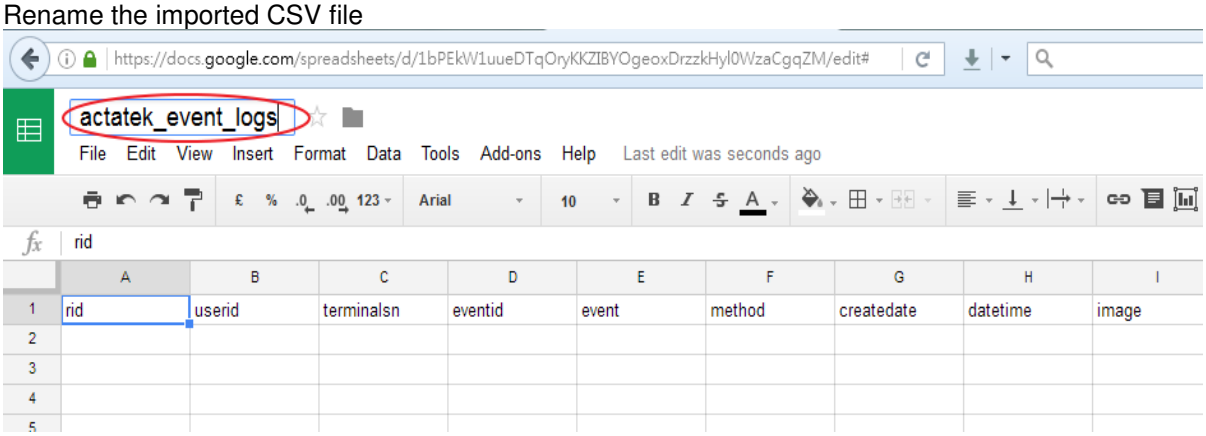
Step3.Download and import the "template event log file" ,and then "open" a new spreadsheet. See below.

Note: Download link of “template eventlog file’
http://www.actatek.com/Downloads/ACTA4/support/template%20eventlog.csv

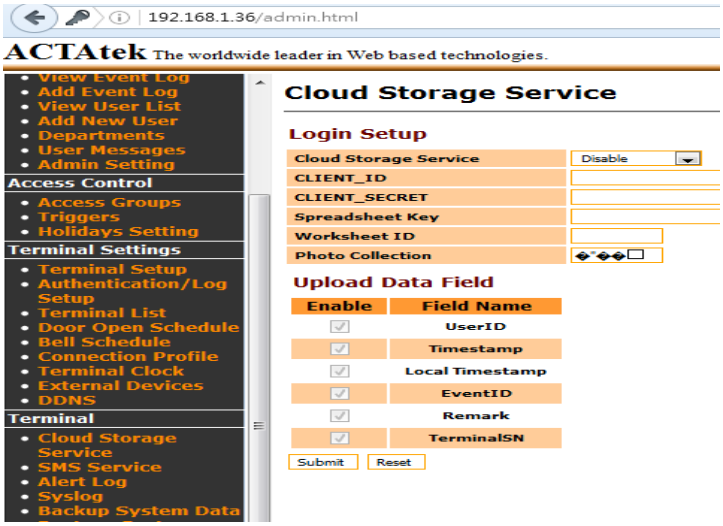




Rename the imported CSV file

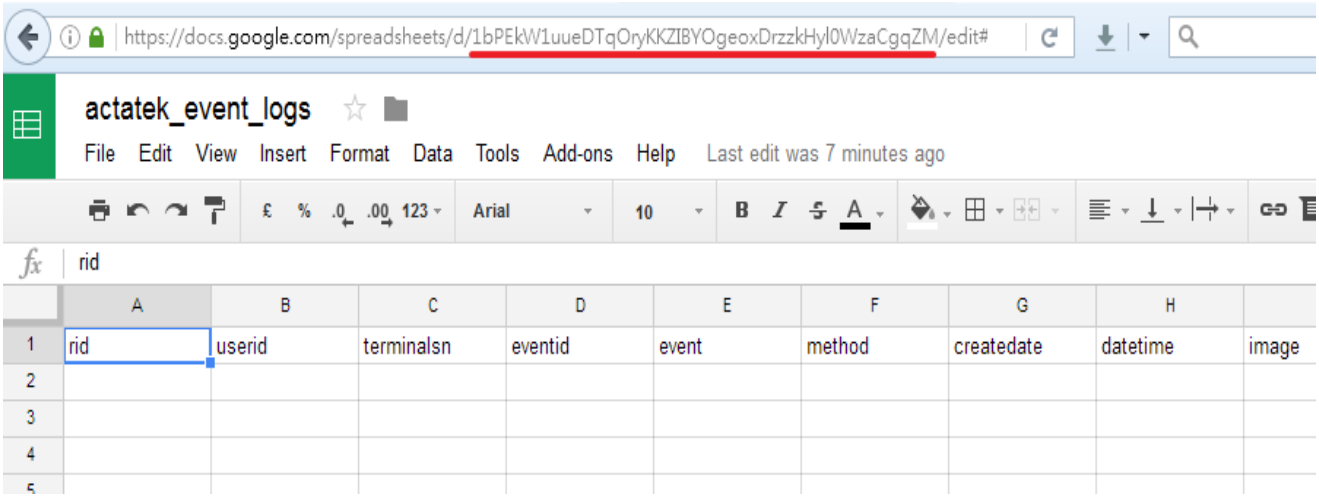


Step4. Login to ACTAtek webpage,and go to [Cloud Storage Service] webpage.



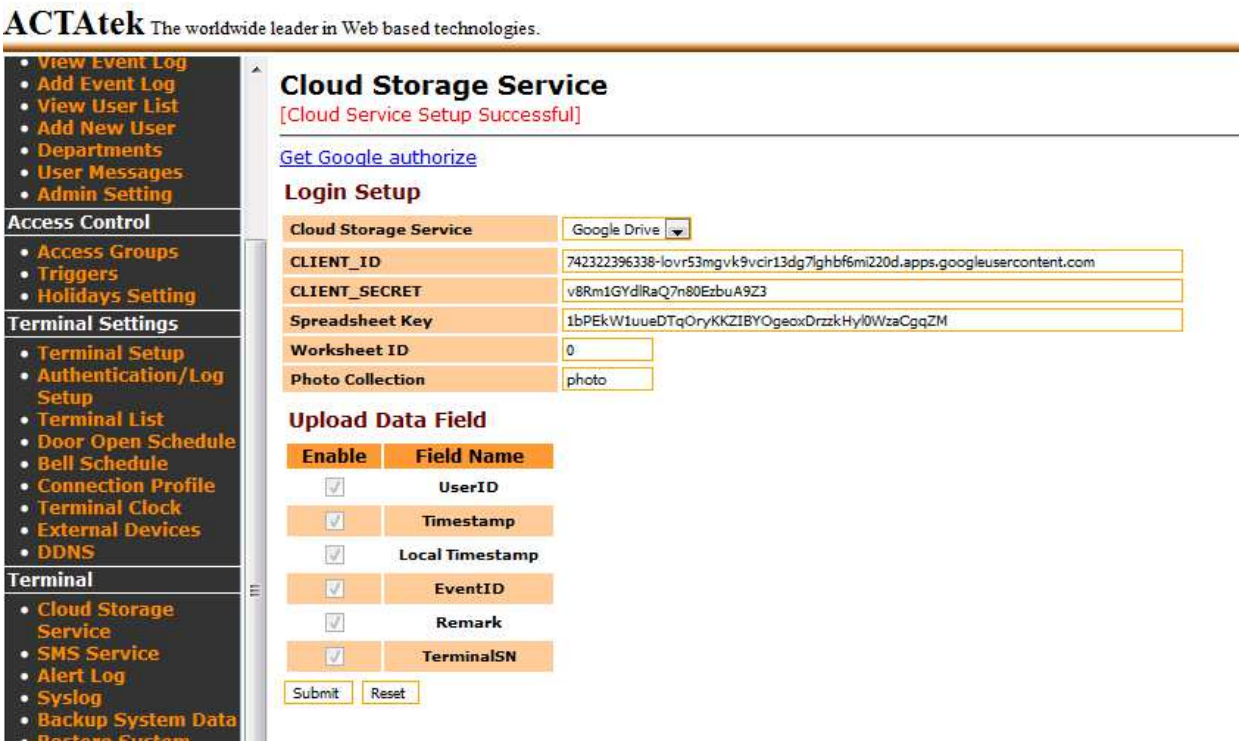
Step5. Select [Google Drive],and then enter the below information, and then click [Submit]

Client ID :742322396338-lovr53mgvk9vcir13dg7lghbf6mi220d.apps.googleusercontent.com
Client Secret:v8Rm1GYdlRaQ7n80EzbuA9Z3
Spreadsheet Key:1bPEkW1uueDTqOryKKZIBYOgeoxDrzzkHyl0WzaCgqZM
(see below as an example)

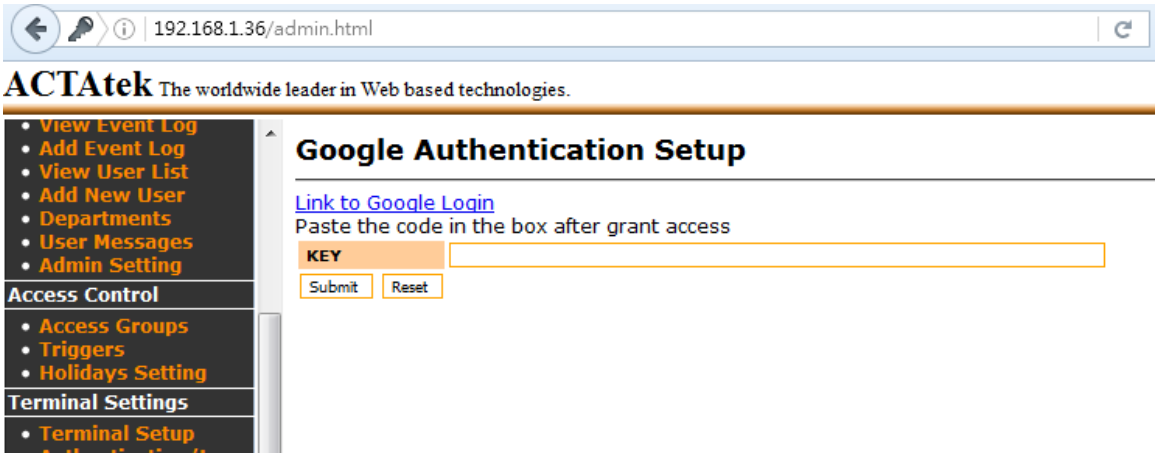


Worksheet ID: 0
Photo Collection: photo

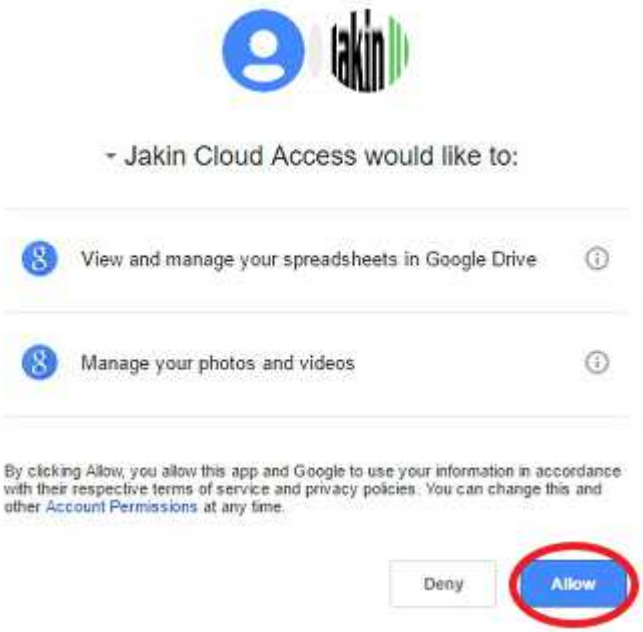
Step6. Click [Get Google authorize] link.
********Make sure that the device's IP settings which were correctly configured, and be able to access Internet.*******



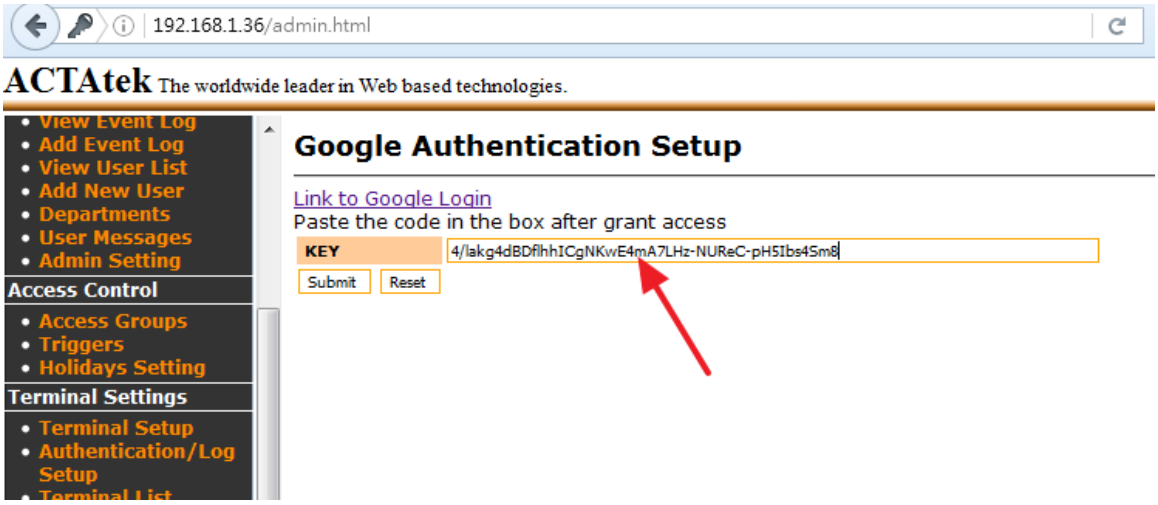
6.1 Click [Link to Google Login] ,and then it will open a new page to ask for the access permission for the device.

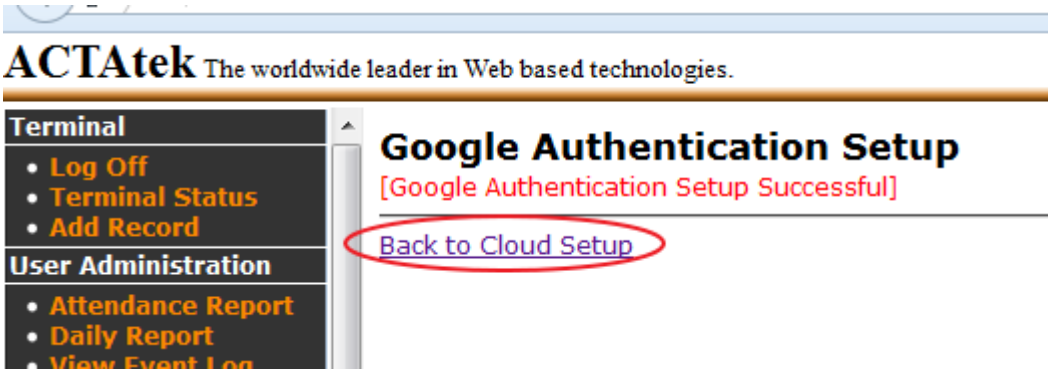


6.2 Click **[Allow]** to grant the access Google Spreadsheets permission for ACTAtek device.

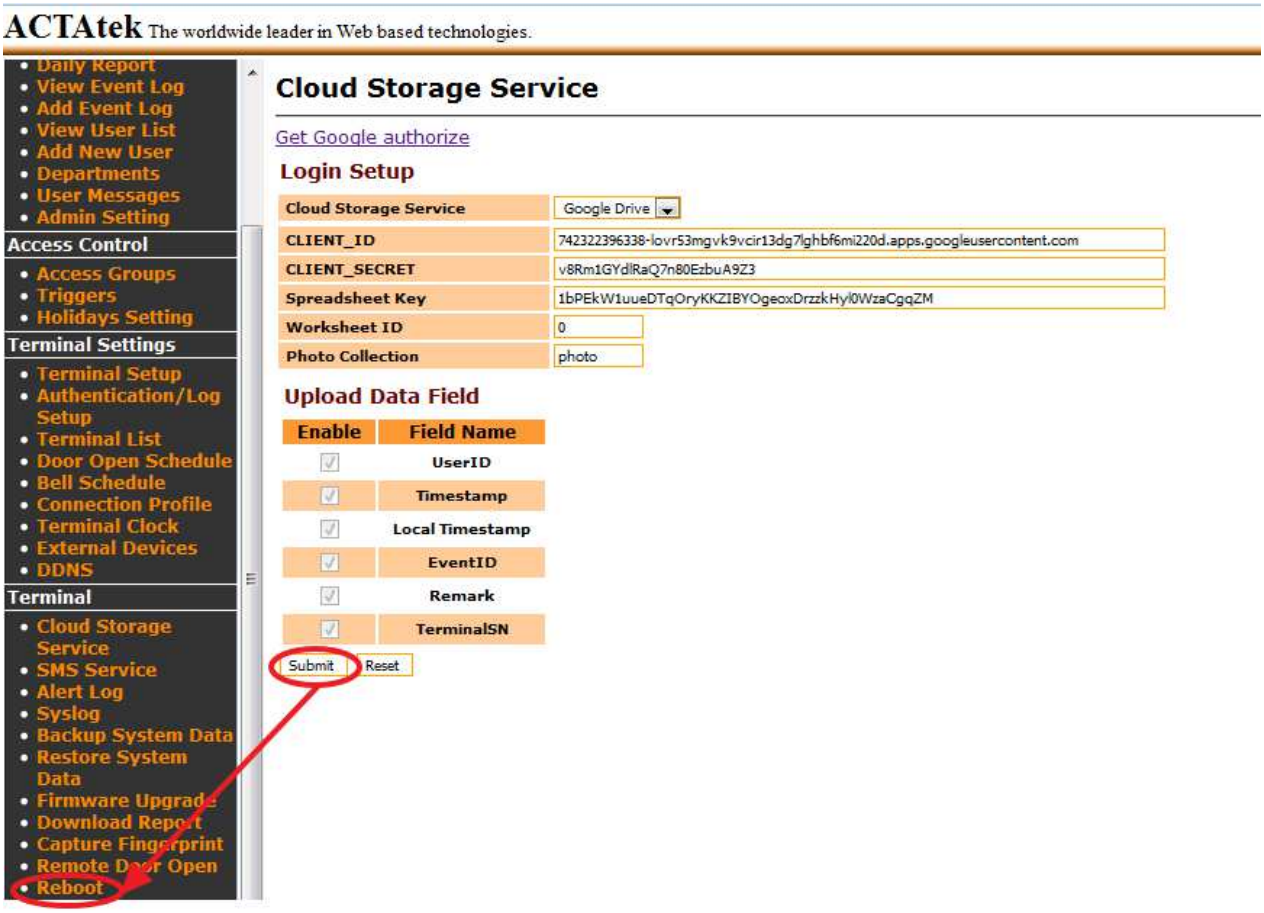


Once done,copy the "**authorized code**" ,and then paste to the device. And then click [Submit],wait for the [**Google Authentication Setup Successful**] message, and then click [**Back to Cloud Setup**]. See below as an example.

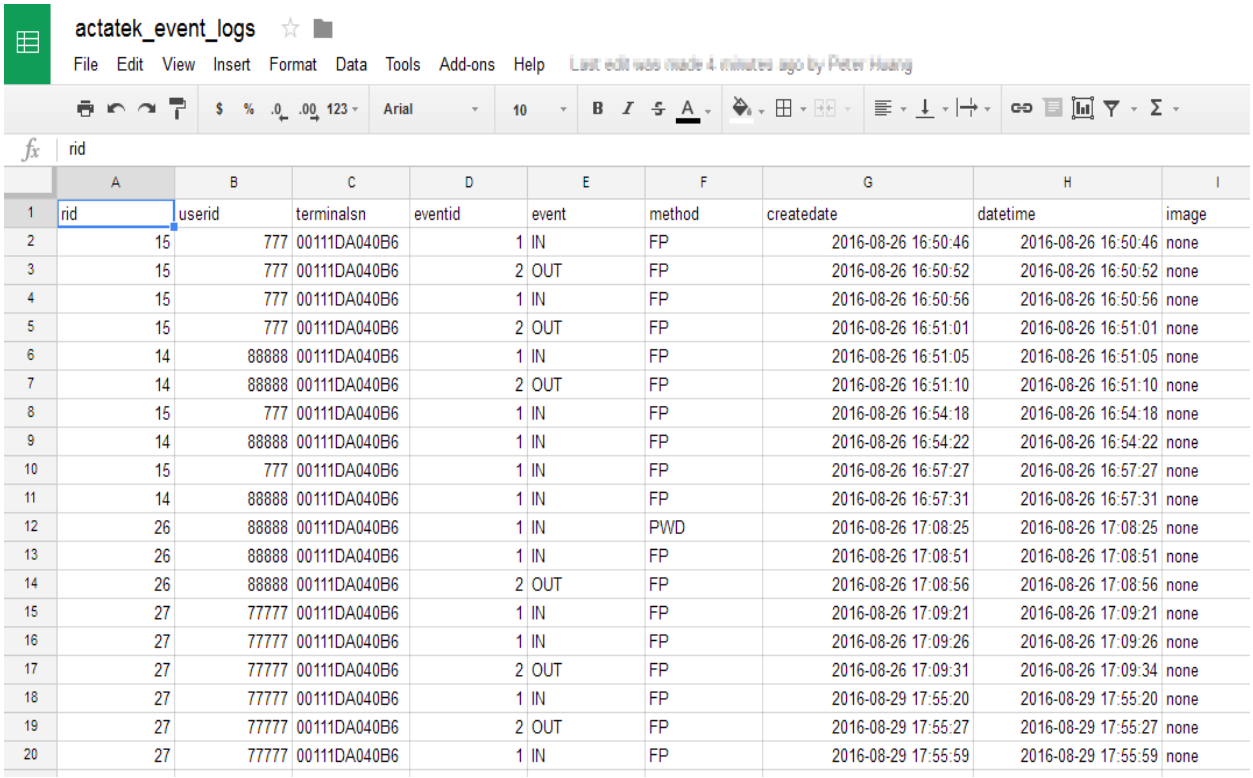




Step7. Click [**Submit**] button once,and then click [**Reboot**] button. After the device was rebooted,the device will start to push the device's Event Logs to the Google Spreadsheets.



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 as an example.



actatek_event_logs

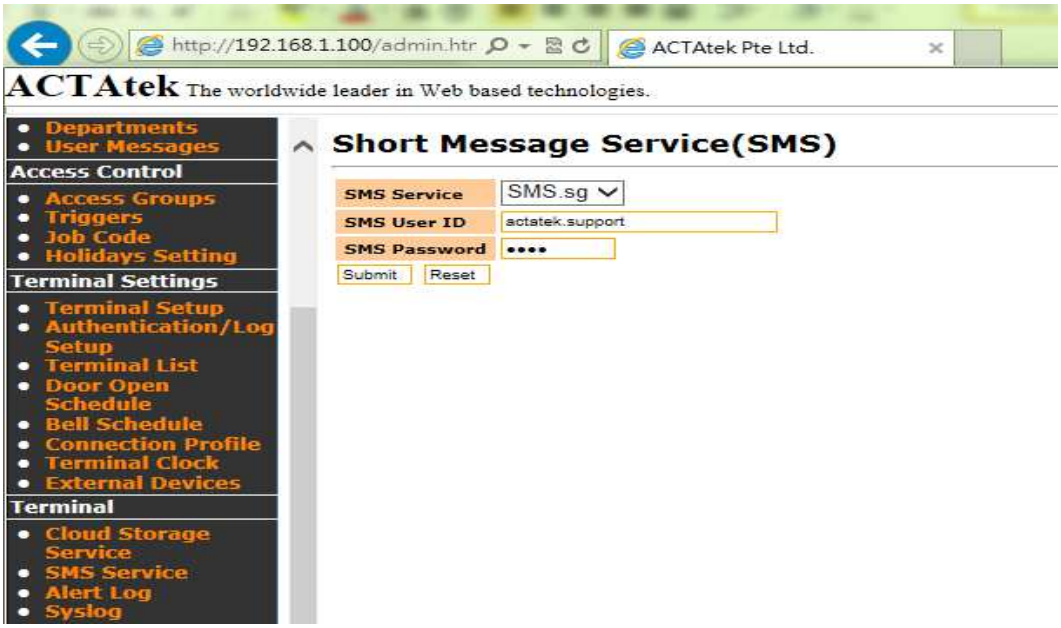
File Edit View Insert Format Data Tools Add-ons Help

fx rid

	A	B	C	D	E	F	G	H	I
1	rid	userid	terminalsn	eventid	event	method	createdate	datetime	image
2	15	777	00111DA040B6	1	IN	FP	2016-08-26 16:50:46	2016-08-26 16:50:46	none
3	15	777	00111DA040B6	2	OUT	FP	2016-08-26 16:50:52	2016-08-26 16:50:52	none
4	15	777	00111DA040B6	1	IN	FP	2016-08-26 16:50:56	2016-08-26 16:50:56	none
5	15	777	00111DA040B6	2	OUT	FP	2016-08-26 16:51:01	2016-08-26 16:51:01	none
6	14	88888	00111DA040B6	1	IN	FP	2016-08-26 16:51:05	2016-08-26 16:51:05	none
7	14	88888	00111DA040B6	2	OUT	FP	2016-08-26 16:51:10	2016-08-26 16:51:10	none
8	15	777	00111DA040B6	1	IN	FP	2016-08-26 16:54:18	2016-08-26 16:54:18	none
9	14	88888	00111DA040B6	1	IN	FP	2016-08-26 16:54:22	2016-08-26 16:54:22	none
10	15	777	00111DA040B6	1	IN	FP	2016-08-26 16:57:27	2016-08-26 16:57:27	none
11	14	88888	00111DA040B6	1	IN	FP	2016-08-26 16:57:31	2016-08-26 16:57:31	none
12	26	88888	00111DA040B6	1	IN	PWD	2016-08-26 17:08:25	2016-08-26 17:08:25	none
13	26	88888	00111DA040B6	1	IN	FP	2016-08-26 17:08:51	2016-08-26 17:08:51	none
14	26	88888	00111DA040B6	2	OUT	FP	2016-08-26 17:08:56	2016-08-26 17:08:56	none
15	27	77777	00111DA040B6	1	IN	FP	2016-08-26 17:09:21	2016-08-26 17:09:21	none
16	27	77777	00111DA040B6	1	IN	FP	2016-08-26 17:09:26	2016-08-26 17:09:26	none
17	27	77777	00111DA040B6	2	OUT	FP	2016-08-26 17:09:31	2016-08-26 17:09:34	none
18	27	77777	00111DA040B6	1	IN	FP	2016-08-29 17:55:20	2016-08-29 17:55:20	none
19	27	77777	00111DA040B6	2	OUT	FP	2016-08-29 17:55:27	2016-08-29 17:55:27	none
20	27	77777	00111DA040B6	1	IN	FP	2016-08-29 17:55:59	2016-08-29 17:55:59	none

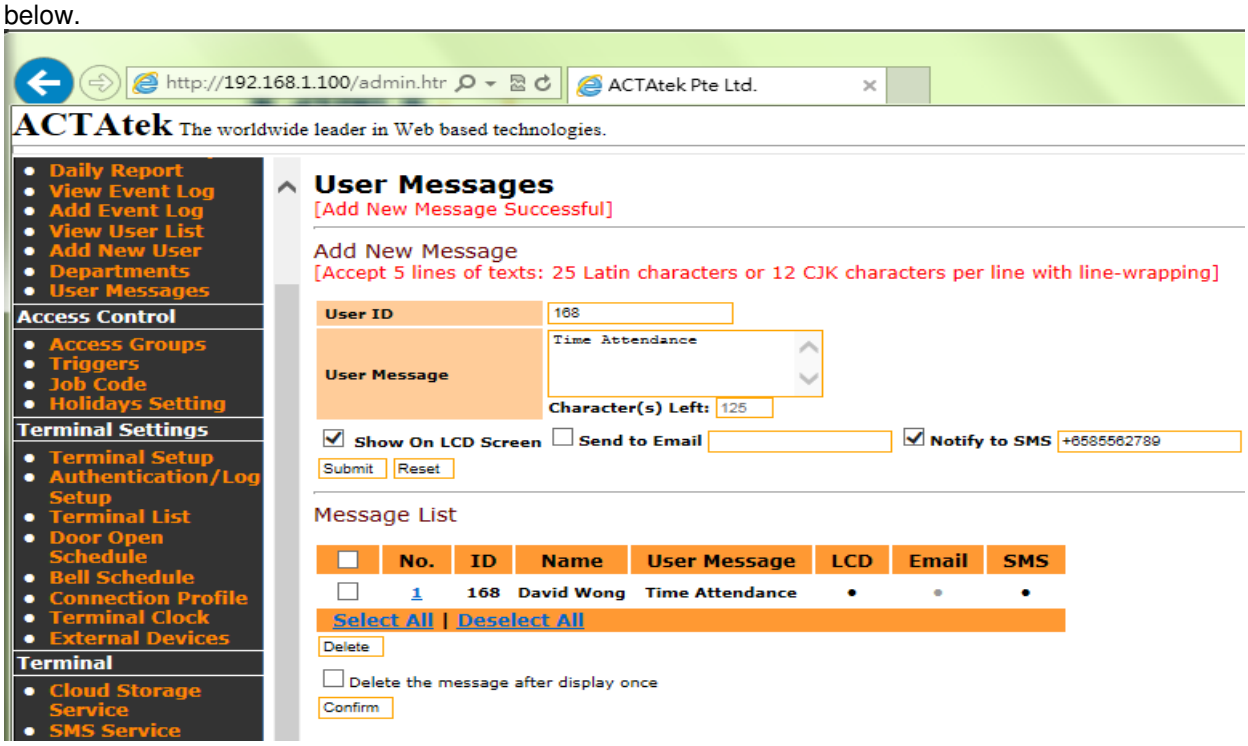
Appendix E. Short Message Service(SMS)

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

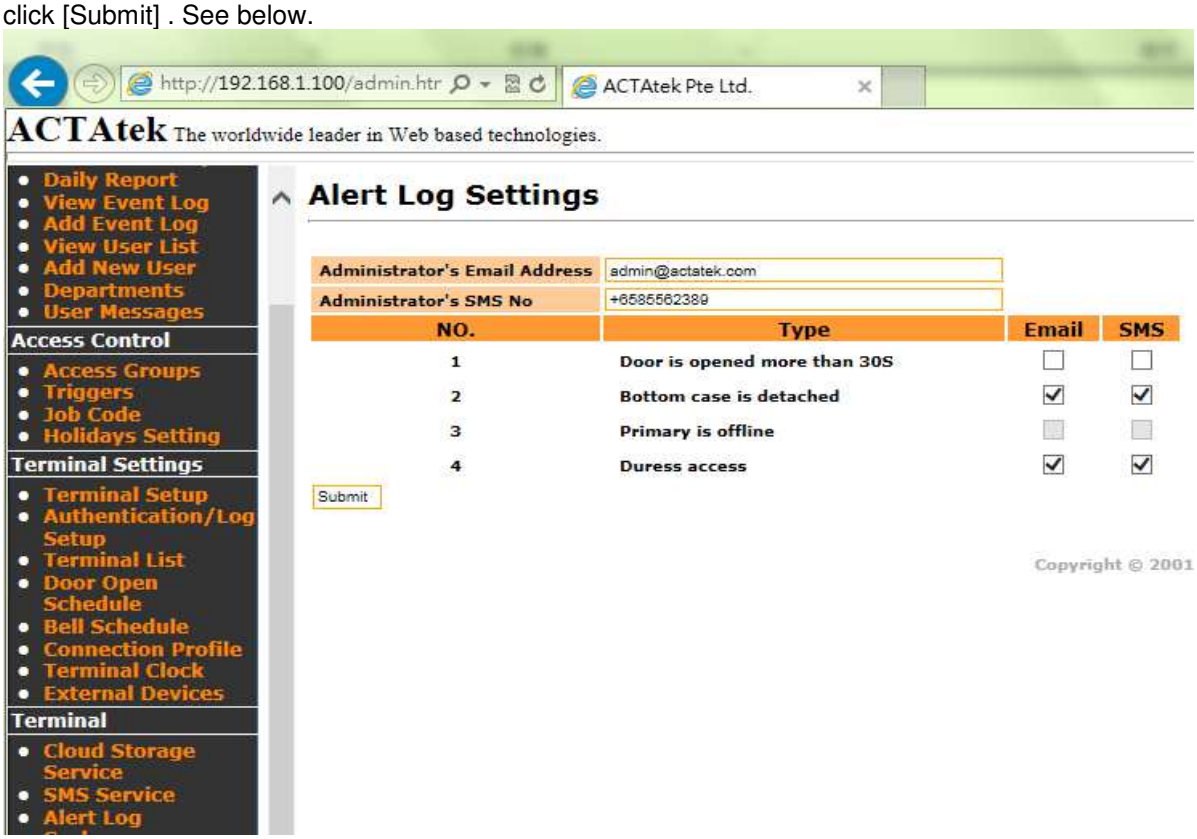


Note1: Make sure that ACTA4's IP settings are correct, and can access the Internet
Note2: The "SMS User ID "and the "SMS Password" can get from http://SMS.SG who provided the SMS Gateway Services. More information can be found at their website at http://SMS.SG

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



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



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.

Appendix F. 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

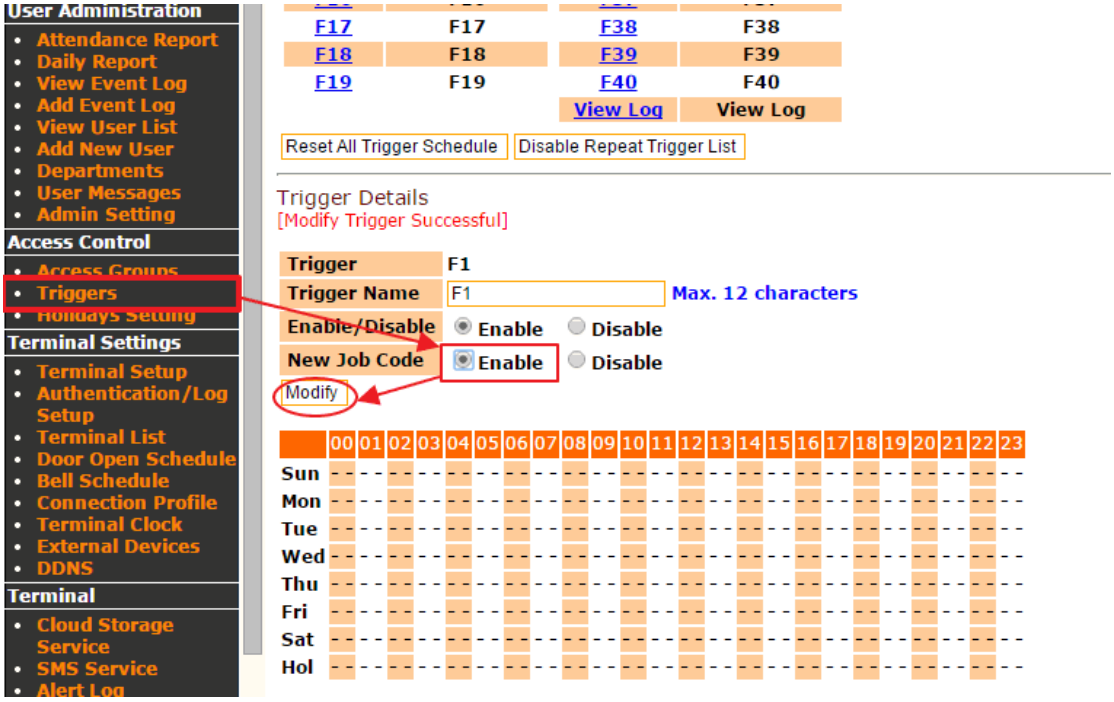
When placing your finger on the scanner, make sure that the location of the "core", located in Step 2, is making direct contact with the scanner. Apply medium pressure, or just enough to flatten the skin on your finger.

Appendix G. Job Costing dialogues (New Job Code)

Job costing dialogues is another 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 Job Code feature. As before, the Job Code feature from ACTAtek is required the admin user to pre-configure the Job Code tables, and its description first to make it work. Now with job costing dialogues feature, the admin user only need to enable this feature and the user can start to use it.

1. Enable New Job Code

To enable job code, please go to [Triggers] ,and click [F1] to enable the feature.



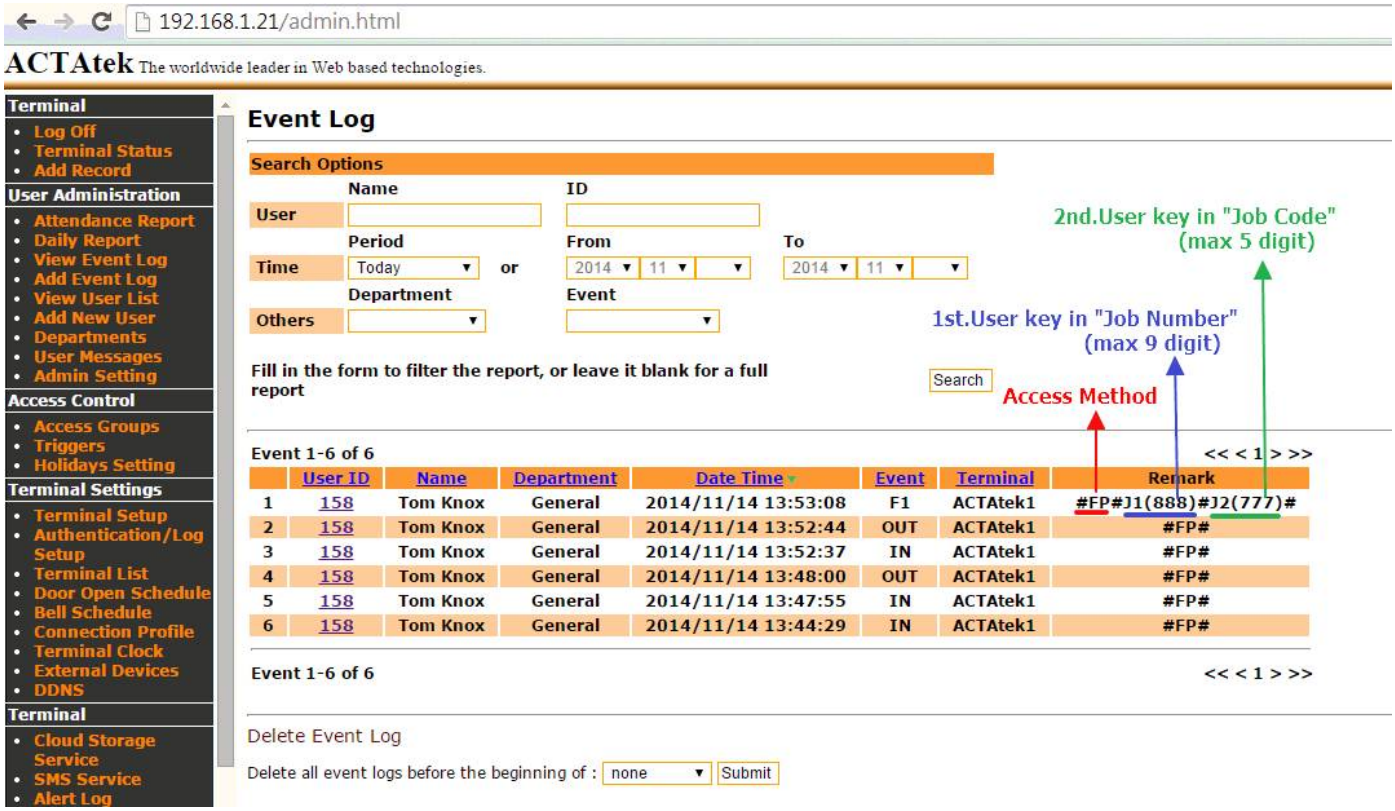
Click [Modify] to enable it..

2. Access the device to enable it

Once the new Job Code was enable,the Users can press [F1] key first to change the device's trigger name to [F1],and then access the device via their enrolled FingePrint/Smart Card or Password . After that,the device's LCD screen will ask the users to key in the first "**Job Number**" (max 9 digit) ,and then press [Enter] key,and then the device will ask to enter the second "**Job Code**" (max 5 digit) to finish their time records together with the users' key-in job costing dialogues info.

3. View the Event Log

When the admin user Login to device's webpage to [View the Event Log] or use the 3rd party's middle-ware to download the Event Logs data,they can use the "remarks field" to check the job costing dialogues info. for their HRMS or PayRoll software integration.



Appendix H. Master/Client Function

With the Master/Client function, customers can configure one device as the **Master terminal** and designate other devices as **Client terminals**.

Once the Client terminals are registered and the Master terminal is ready, the Master–Client devices will automatically synchronize data with each other. This includes:

- User fingerprint (FP) data
- Event log data
- Other relevant system records

Refer to the system diagram below for an overview of the configuration.

Master/Client Setup Procedure:

1.Enable Master Mode

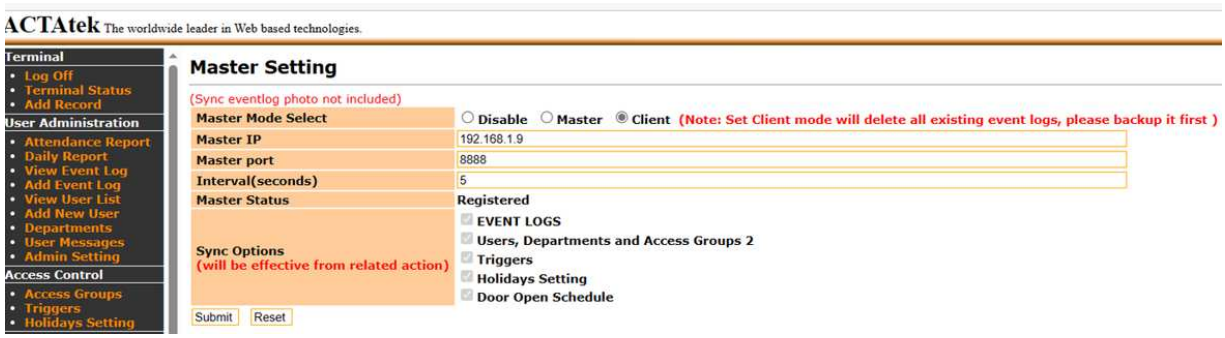
- Log in to the Master device.
- Navigate to the **[Master/Client Setup]** page.
- Select **[Master]** mode and click **[Submit]** to apply the setting.

2.Enable Client Mode

- Log in to each Client device.
- Navigate to the **[Master/Client Setup]** page.
- Select **[Client]** mode.
- Enter the **[Master IP]** address.
- Click **[Submit]** to apply the setting.
- The Client device will then upload and download data from the Master device and automatically reboot.

Verify Registration

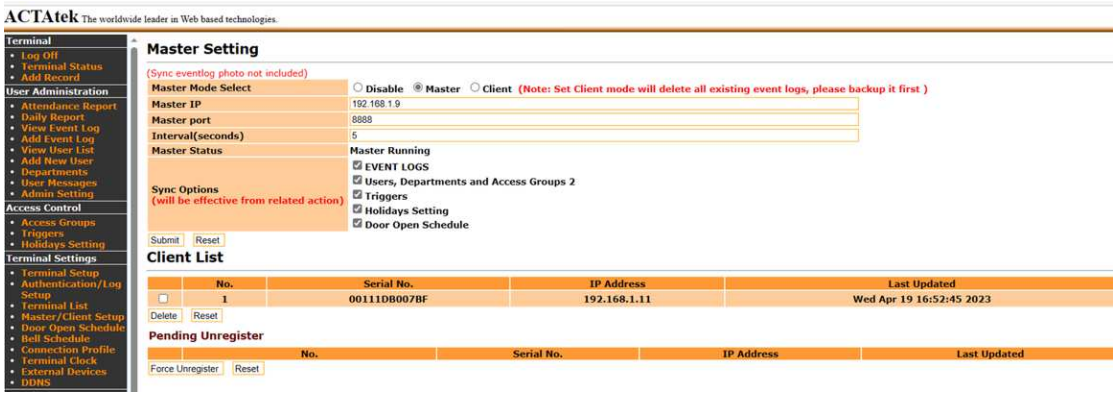
- After reboot, the Client device will display **[Registered]** under **[Master Status]**, indicating successful synchronization and readiness.



Note:

1. A Client device can operate in either **[Standalone]** mode (via Master/Client setup) or **[Access Manager]** mode.
2. One Master device supports up to **10 Client devices** registered simultaneously.

Master Device:
The client list displays all registered client devices.



Event Logs:
All event log data will be synchronized across both Master and Client devices.

Event 1-10 of 10 << < 1 > >>

	User ID	Name	Department	Date Time	Event	Terminal	Remark
1	8899	- -	General	2023/04/19 16:59:15	IN	00111DB007BF	#FP#
2	8899	- -	General	2023/04/19 16:59:00	OUT	Main	#FP#
3	8899	- -	General	2023/04/19 16:58:53	IN	Main	#FP#
4	8899	- -	General	2023/04/19 16:58:42	OUT	00111DB007BF	#FP#
5	77777	TEST MYSQL	General	2023/04/19 16:56:38	OUT	Main	#FP#
6	8899	- -	General	2023/04/19 16:56:34	IN	Main	#FP#

Appendix I. ACTA4 Intercom.

Introduction

Acta4's intercom function can talk to PC or smart phone if all parties are in the same intranet. Below is the descriptions of the setup of Acta4 SIP based intercom to talk with PC or smart phone using third party SIP client phone.

SIP Phone Setup Procedures

Step A :- PC or Smartphone

1. Download and install Linphone on your PC

http://www.linphone.org/releases/windows/Linphone-4.1.1-win32.exe

2. Download and install Linphone on your smart phone by going to App store and search for "Linphone"

Step B :- Acta4

1. Login to Acta4 web portal, eg, 192.168.1.104

2. Click "Intercom" on the menu on left hand side (see below picture).

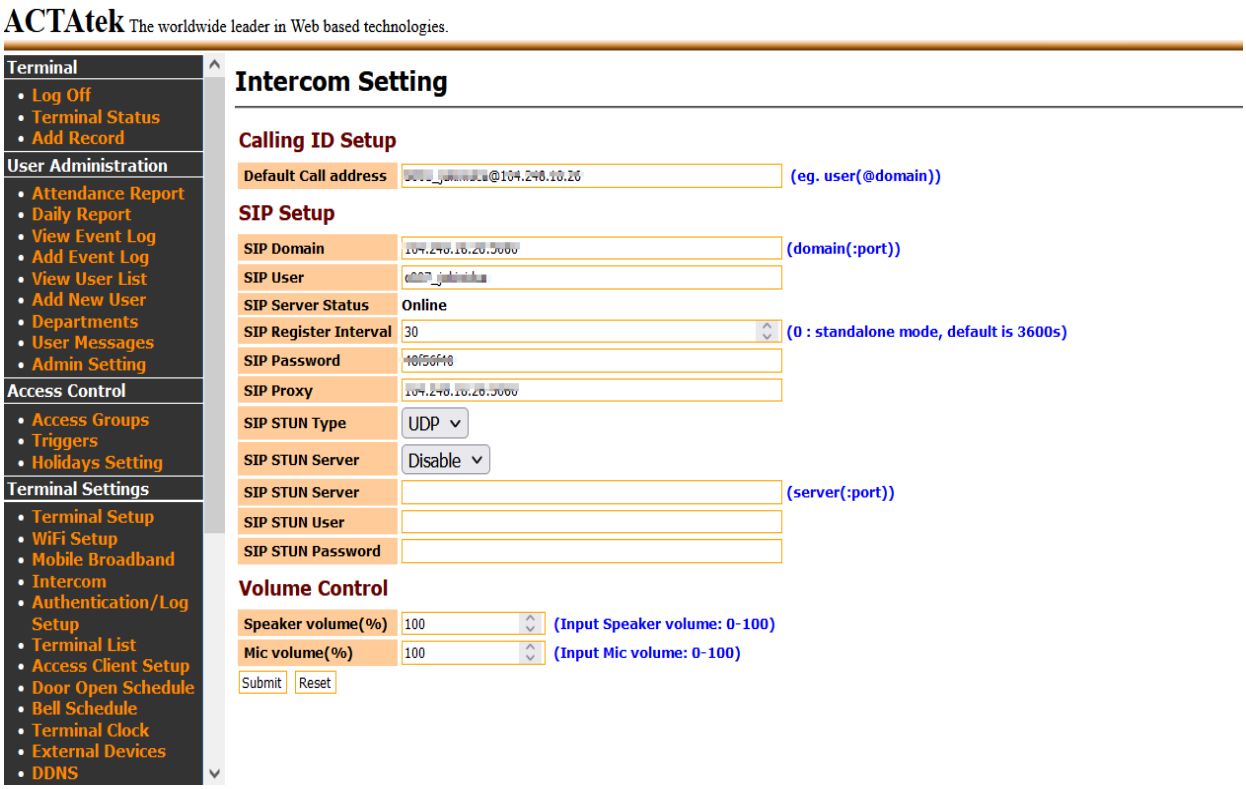
3. Input the SIP IP of the party you want to call from this Acta4 terminal. Eg, if you want to call to the PC which already installed Linphone with IP address 192.168.111.85, then just input that PC's SIP IP as: jakinidpc@192.168.1.10:5060 where "jakinidpc" is the user name of the PC, which can be arbitrary.

4. Input the speaker volume of the intercom from 0 to 100%, you can change this value at any time during intercom conversation.

5. Input the mic volume of the intercom from 0 to 100%, you can change this value at any time during intercom conversation.

6. Click "Submit" to save. Then you can make call from Acta4 at any time (see next chapter)

Note:If the client side has its own SIP server internally, please consultant with the IT network team about the SIP server's configuration settings in details.



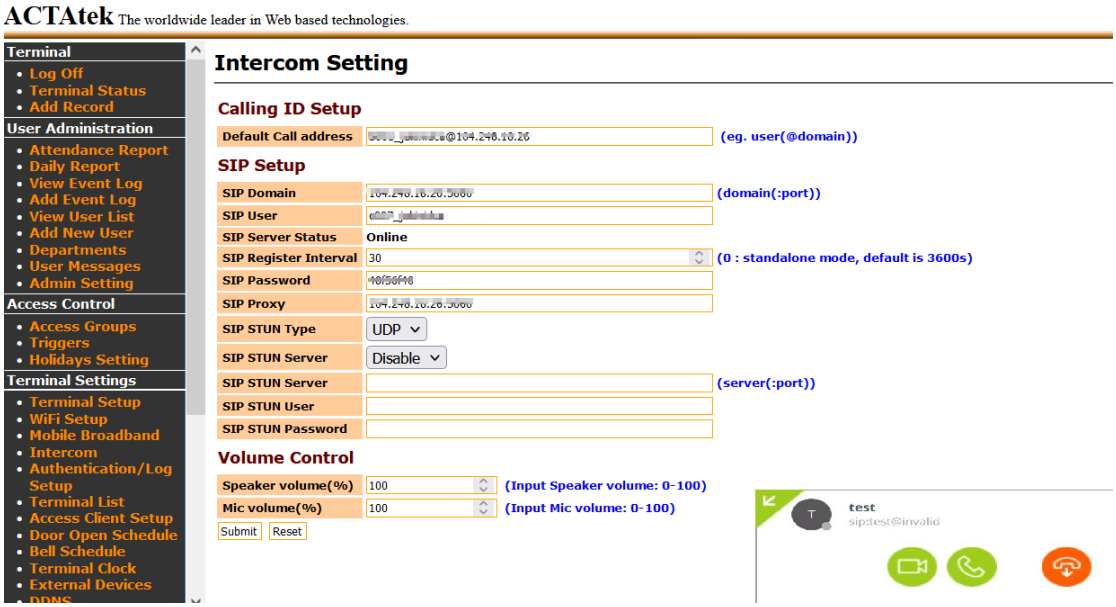
Making Call

From Acta4 to PC/Smartphone

1. Make sure the Linphone is running on your PC.

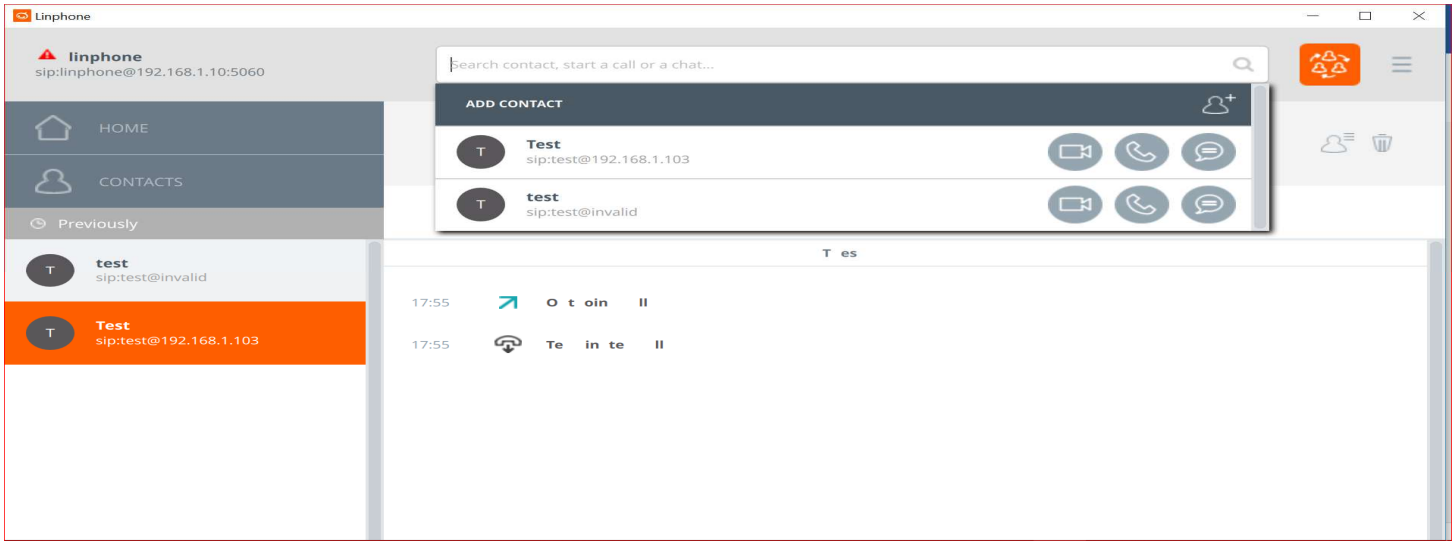
2. Press the “bell” button on the Acta4 to make a call to the PC.

3. A window will have popped up in the bottom right of your PC showing a call from Acta4.



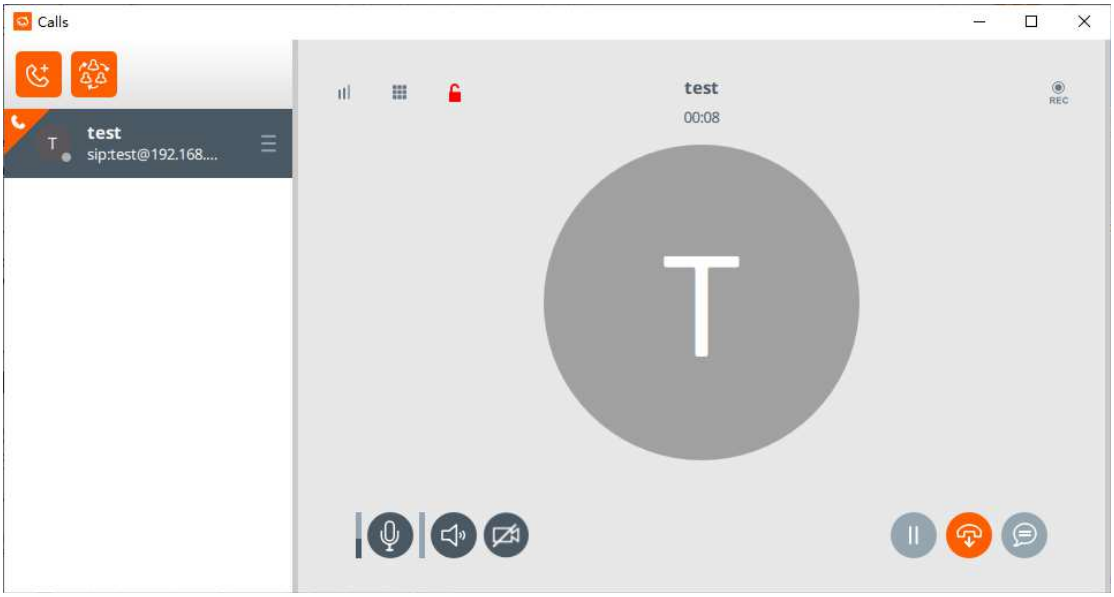
From PC/Smartphone to Acta4

1. Open the Linphone and input SIP IP of the Acta4 you want to call to. Note that it MUST be in the format: sip:test@xxxxxxxx, where “xxxxxxxx” is the IP of the Acta4.



3. A window popped up immediately on the PC to show that the call to Acta4 is connected successfully.

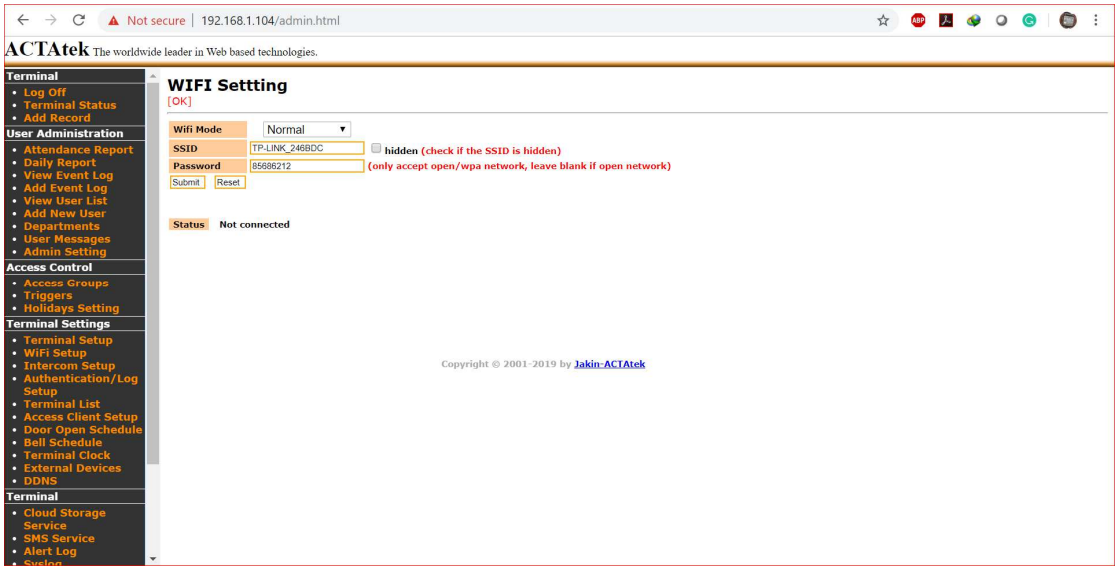
3. You can press the red button in the window to terminate the call. (Note that you cann't terminate the call in Acta4)

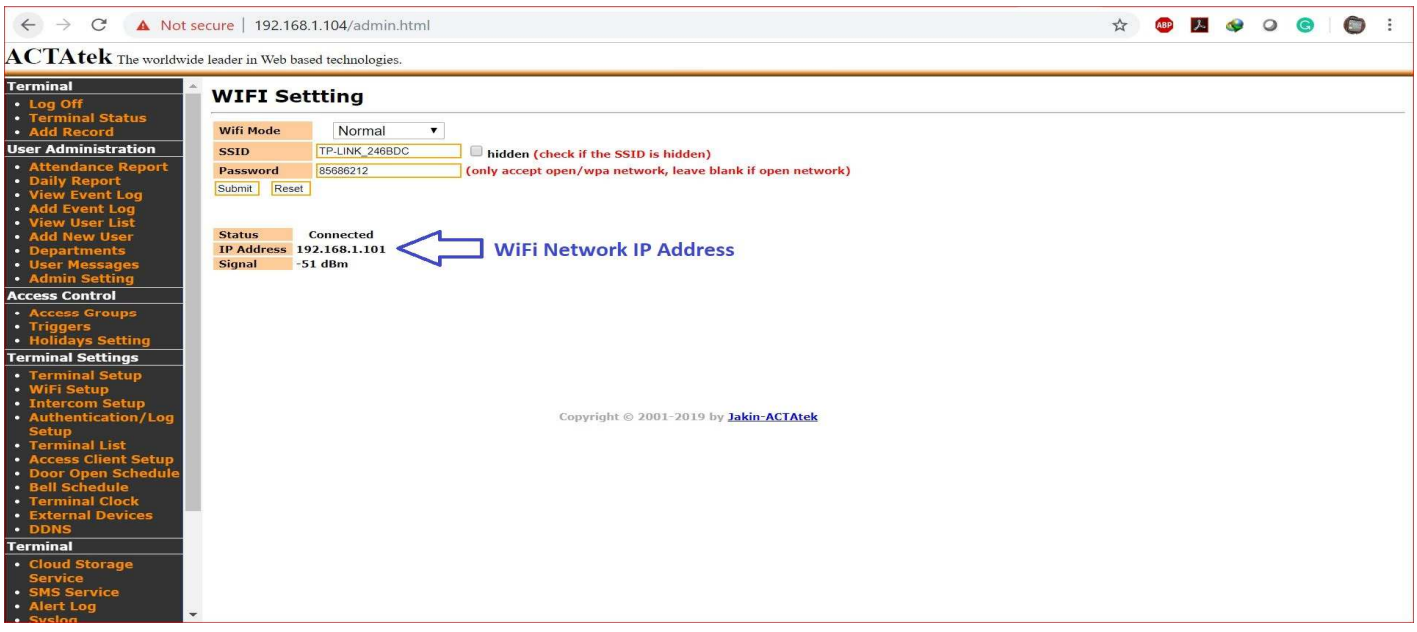


Appendix I. ACTA4 WiFi-Setup

WiFi mode: Normal

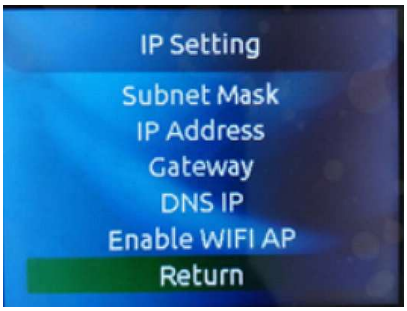
1. Login to Acta4 web portal, eg, 192.168.1.104
2. Click “WiFi Setup” on the menu on left hand side (see below picture).
3. Select WiFi mode as ‘Normal’ to connect with a WiFi network.
4. Input the SSID and password.
5. Click “Submit” to save. Then refresh the page to get the ACTA4 NIC IP address of WiFi network. The user can also obtain the WiFi IP address by pressing the physical device’s ENTER key button 6 times to check the Device Info. Page.



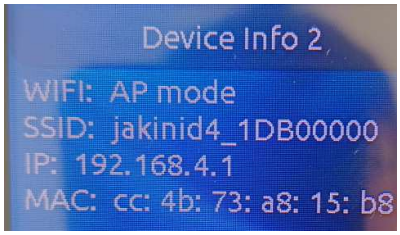


WiFi mode: AP(AccessPoint)

1. Press the physical device [Admin Login] menu button on the keypad of your ACTA4 unit.
2. The system will prompt for the Admin ID. Please enter the default one: A999,
3. Press Enter / Return
4. The system will prompt for the Password. (Default: 1)
5. Press Enter / Return, and you will see the Administration Menu.
6. Select the icon on the bottom left of the screen, which is for IP Settings.
7. Press 'Enter/Return' once IP Settings is highlighted.
8. Press the 'Previous/Next' buttons to highlight "Enable WiFi AP", press 'Enter/Return'.



9. Open your mobile phone's WiFi , and connect to the WiFi SSID of ACTA4 device e.g. jakinid4_1DB00XXX,and enter the WiFi password **jakinid4**.
10. After connecting to the ACTAtek device under WiFi AP mode successfully, please press ENTER key button 6 times to check the Device Info. page, and then press > key button to see the Device Info.2 page where you can find the device's IP addtess.e.g.IP:192.168.4.1



11. After that you can open browser to access the device's webpage at 192.168.4.1.

Appendix J. ACTA4 WiFi connection setup

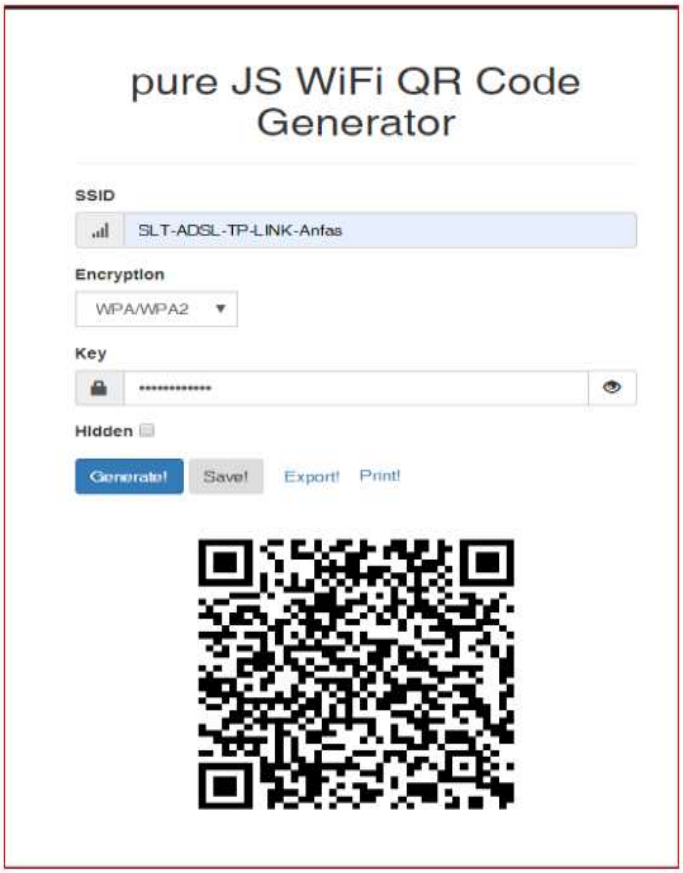
The Super Administrator can Login to ACTA4 device's console menu to use "Scan WIFI QR Code" function under Networking setting sub-menu.

This function can convert the customer's WiFi connection credentials to a "QR code", and then use this QR code to be scanned at ACTA4 for auto- configure the device's WiFi settings.

Upon the credentials are correct, the ACTA4 will automatically connect to the customer's WiFi access point, and becomes as wireless connection.

See below website link as an example which it will help make a WiFi QR Code at your mobile's browser first, and then scan at ACTA4 device.

https://qifi.org/



Appendix K. ACTA4 4G connection setup

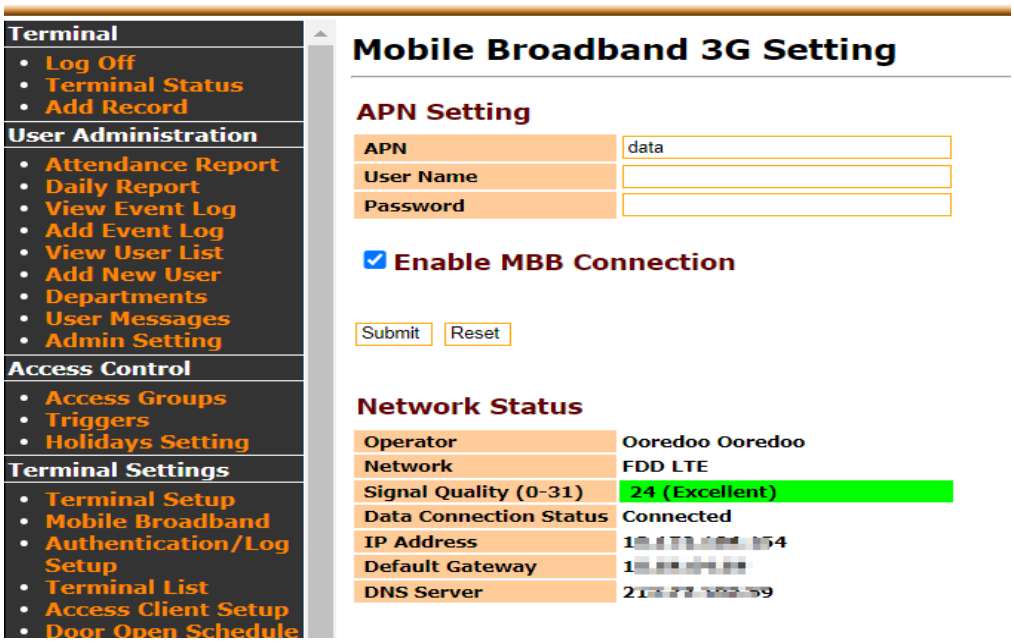
Step 1.Removal of the device's back case, and then remove the wiring board to insert the SIM card.

YouTube https://www.youtube.com/watch?v=JOUnDCRw-ig

Step 2.Login to device's web-page, and then click "Mobile Broadband", in APN Setting, enter the APN name (*you should be able to get the APN name from your local Telecom operator), leave the Username and Password blank.

Step 3. Check the "Enable MBB Connection" to enable data connection

Step 4. click "Submit" then the 4G modem will dial-up for mobile broadband connection.



Step 5. You can check whether mobile broadband connection is successful or not by clicking the "Mobile Broadband" multiple times until the "Connection Status" shows "Connected" ,and the IP will also shown. Or you can check it from the physical device's device info. page.

Appendix L. How to use QR code to access ACTAtek device?

Option 1.Normal QR code

QR code is like another type of digital password so that the customer can purchase any ACTAtek device with the built-in camera function to support it. e.g.ACTA4-1K-**P**-**C** (*PIN model with built-in camera) which means that it does not need to have Facial model or Smart Card model to make it work.

As for the generation of QR code, please either Login to **ACTAtek device** or **AMS webpage** to enter any numbers or strings of characters to generate a QR code. See the attached file as examples.

Note:For AMS or AMS SaaS, the QR code icon will not show up until a Smart Card number is entered/saved.

After that, please save the generated QR code as a JPEG file, and then send it to User's mobile phone via WhatsApp or email attachment file or print it out . See below steps as an example about how to generate a QR code ,and then access the device.

Work flow of adding QR code user from the device's webpage:

1.Login to device's [Add New User] page or [View User List] page, and then enter User's preferred QR code number e.g.20210210 or use the existing smart card no. to generate .
2.Enable 'Smart Card' status.
3.Click 'Add' or 'Modify' button to save the above User's QR code settings.
4.Click 'Show QR code.
5.You can then use the right-click to save the generated QR code as a JPEG file,and then transfer the JPEG to your mobile phone or print it out to access the device. After accessing the device via User's QR code, the device's LCD will display 'Please remove QR-Code' ,and then also capture User's picture.

Note:
1.Please keep **at least 20 cm** distance when accessing the device from mobile device's saved QR code.
2.As for the printed hardcopy of QR code ,please ensure that the QR code size is **3.5 CM * 3.5 CM** .


Access Group
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
Production
Sales
SmartCard/QRcode Number
Show QRcode
Activate Read
Capture Fingerprint
Activate Capture
Fingerprint Security Level (for ID Match)
Normal
Status
Active
Auto Match
Password
Smart Card
Fingerprint
Group ID:
Expiry Date
Disable
Enable
(yyyy/mm/dd)
First Lunch IN Time
Reset
Modify
Clear
genQRcode.cgi (740×740) - Microsoft Edge
192.168.1.7/cgi-bin/genQRcode.cgi?s=888777demo
Copyright © 2001-2022 by Jakin-ACTAtek
ACCESS MANAGER SUITE
Welcome admin ! [Log Out]
Home
Access Manager
Access Application
Control Panel
About
ACCESS MANAGER
Site
Location
User
Add User
View/Edit User
Bulk Edit User
Department
Access Group and Access Right
Trigger and Holiday
Door and Bell Schedule
Event Log
Terminal
View Terminal
Open Door by Terminal
Copy Terminal User
Copy Terminal Access Right
Copy Terminal Trigger
Associate Location
Associate Terminal
Associate Department
VIEW / EDIT USER
User Status
Number of users in system: 22 [Editable: 22]
Export
File Format:
TXT
Export
General
Department/Access Group
Details
Site/Location
General
User ID
Password
Smart Card
QR Code
Facial Template Image
First Name
Other Name
Last Name
Administrator Level
Finger Print Security Level
Finger Print Type
Status
Active
Password
Finger Print Automatch
Finger Print
Facial Automatch
Facial
Smart Card
Finger Print Group
Notification
ACTAtek The worldwide leader in Web based technologies.
Terminal
Log Off
Terminal Status
Add Record
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
WiFi Setup
Intercom
Authentication/Log Setup
Terminal List
Access Client Setup
Door Open Schedule
Bell Schedule
Terminal Clock
Event Log
Search Options
Name
ID
User
Period
From
To
Time
Today
or
Department
Event
Others
Fill in the form to filter the report, or leave it blank for a full report
Search
User-defined QR code
Event 1-6 of 6
<< < 1 > >>
User ID
Name
Department
Date Time
Event
Terminal
Captured Image
Remark
1 8888 Demo User General 2023/01/30 10:47:58 IN ACTAtek View Image #SMC(SN:20201106demo)#
2 8888 Demo User General 2023/01/30 10:47:40 IN ACTAtek View Image #SMC(SN:20201106demo)#
3 8888 Demo User General 2023/01/30 10:47:12 IN ACTAtek View Image #SMC(SN:20201106demo)#
4 A11231 Smith Jhon General 2023/01/30 10:47:01 IN ACTAtek View Image #SMC(SN:123455)#
5 A11231 Smith Jhon General 2023/01/30 10:43:27 IN ACTAtek View Image #SMC(SN:123455)#
6 A11231 Smith Jhon General 2023/01/30 10:43:02 IN ACTAtek View Image #SMC(SN:123455)#
Event 1-6 of 6
<< < 1 > >>

Option 2. Two-factor authentication (Google Passcode)

Google Authenticator is a mobile app that generates verification codes for 2-Step Verification, adding an extra layer of security to your QR Code User account. You can use Google Authenticator to sign in to your ACTAtek account with a QR code, instead of entering a password.

Here are the steps to create a QR code user with Google Authenticator Key on ACTAtek or AMS:

1. Download and install the Google Authenticator app on your smartphone. You can find it on the Google Play Store for Android devices or the App Store for iOS devices.

2. Login to ACTAtek WEB UI and go to **"Authentication Log Setup"** and then enable **"Gauth Mode"** as 2Fector Authentication.

3. Log in to your ACTAtek or AMS account on your computer. Go to the user account section and click the KEY button next to the G Authenticator Key to enable the passcode key.

4. A QR code will be generated and displayed on the screen for G Authenticator.

5. Open the Google Authenticator app on your smartphone and tap on the plus icon (+) at the bottom right corner. Choose Scan a QR code and point your camera at the G Authenticator QR code on your computer screen. The app will scan the code and add your ACTAtek or AMS account to the list of accounts.

6. Click on Save User to finish creating the QR code user. You can now share the QR code with the end user by sending it via email, printing it, or saving it as an image file.

7. Scan the QR code at ACTAtek device and it will ask you to enter the 6-digit passcode. Now open the app on your smartphone and enter the verification code that appears next to your account name. The access will be granted when both credentials (QR+Passcode) are matched. Please check the sample events in below attachment.

Note:

1. For AMS or AMS SaaS, the QR code icon will not show up until a Smart Card number is entered/saved.

2. Please keep at least 20 cm distance when accessing the device from mobile device's saved QR code.

3. As for the printed hardcopy of QR code, please ensure that the QR code size is 3.5 CM * 3.5 CM.