# Web Server 3.0

## User Manual

# Preface

Without the permission of ZKSoftware INC., any copy is prohibited.

All the specifications of the products mentioned here are subjected to the real objects. The company does not undertake that the real products are consistent with the information. The company does not undertake any dispute caused by the disagreement of actual technical parameter and this information. Besides, the company is not responsible to notice in advance.

The other brand and product mentioned in this file mean the company（possessing corresponding brand and product）or its manufactured products。The company does not possess any privilege of the brand and product belonging to other companies.

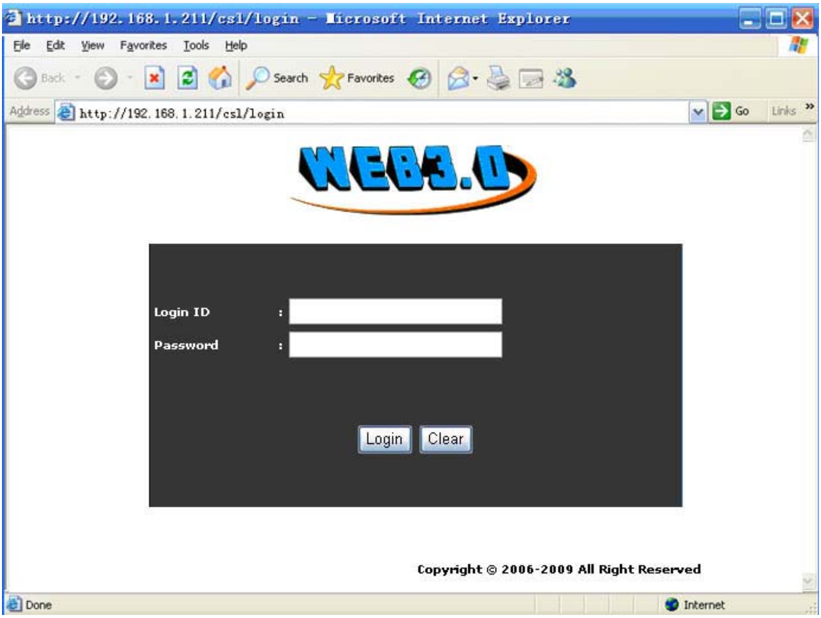
Remote data capturing system on Web Server is based on TCP/IP standard network structure. WEB page request is adopted to process and manage data. It is out of region restriction and it is not necessary to install other software. It can download and manage the data in fingerprint terminal remotely online through IE, NETSCAPE and other browsers. Then it makes various statistic statements for enterprise management and decision-making, achieving information synchronized any time any where and realizing high-efficient management.

# CONTENTS

# 1. Log in Web Server

1、When Web Server is used, device's IP address should be set firstly.

2. Input http://192.168.1.211 in IE address column. Press ENTER to get the following picture:


http://192.168.1.211/csl/login - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address http://192.168.1.211/csl/login
Go Links
WEB3.0
Login ID :
Password :
Login Clear
Copyright © 2006-2009 All Right Reserved
Done
Internet

3. To ensure system safe, ID verification needs to be done before entering system. The default account of super administrator: administrator; password: 123456 (which can be modified after entering the system).

**Notice:**

1. The administrator account can’t be modified.
2. The password can be modified. Capital & small letters are used for password. The way to modify, please refer to 6.4 Password.

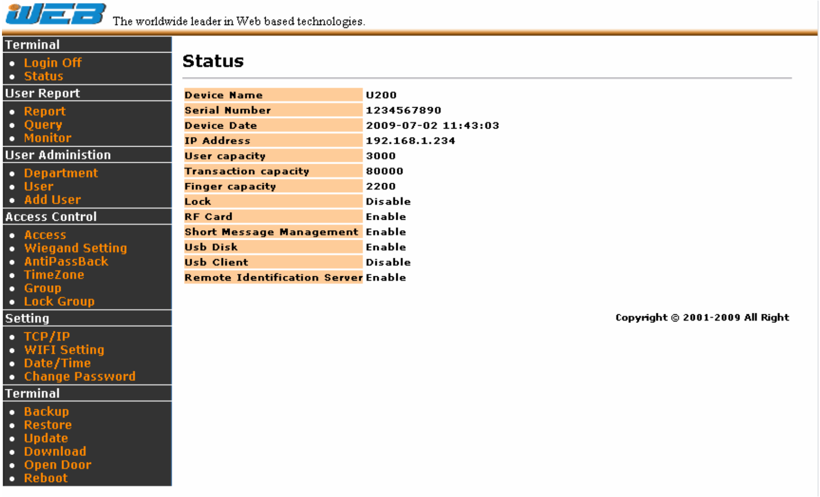
# 2. System Management

## 2.1 Exit from Web Server

If you want to exit from the system, click “Terminal” → “Login off” to exit to the login in window.

## 2.2 Device Status

After entering into Web Server, system will display the basic information and the statuses of some functions about this device. Or click “Terminal” → “Status” as below shown:



**Status**

| | |
|---|---|
| Device Name | U200 |
| Serial Number | 1234567890 |
| Device Date | 2009-07-02 11:43:03 |
| IP Address | 192.168.1.234 |
| User capacity | 3000 |
| Transaction capacity | 80000 |
| Finger capacity | 2200 |
| Lock | Disable |
| RF Card | Enable |
| Short Message Management | Enable |
| Usb Disk | Enable |
| Usb Client | Disable |
| Remote Identification Server | Enable |

Copyright © 2001-2009 All Right

The device information includes: device name, serial number, device date, IP address, user capacity, record capacity, finger capacity; as well as the status information of some functions.

**Notice:**

1. After modifying the information of device such as IP address etc., it is required to restart the device, then view the relate information of the device by visiting the web server.
2. When there is no access control function in device, the ‘Lock’ in Status will display ‘Disable’, and the ‘Access Control’ in left menu column will hide automatically.

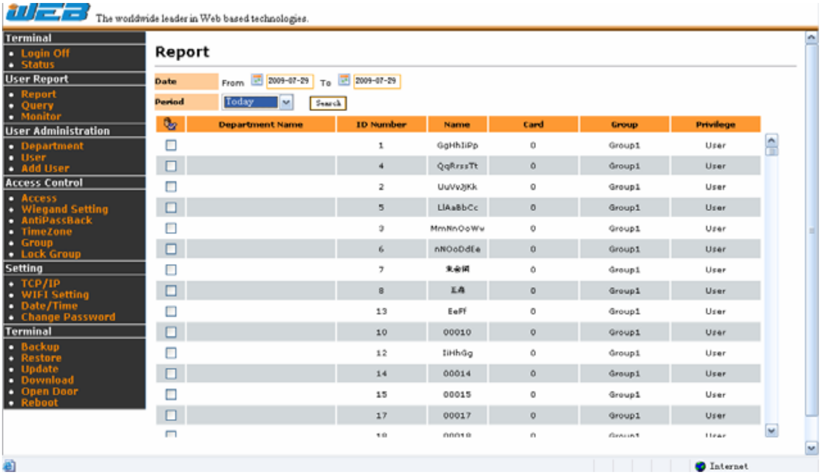
# 3. User report

## 3.1 Export the report

**[function introduction]** export in&out records of specified personnel during some period.

**[operating steps]**

1. Click "User report"→"Report" to open the Report page:



Report

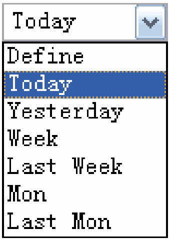
Date From 2009-07-29 To 2009-07-29

Period Today

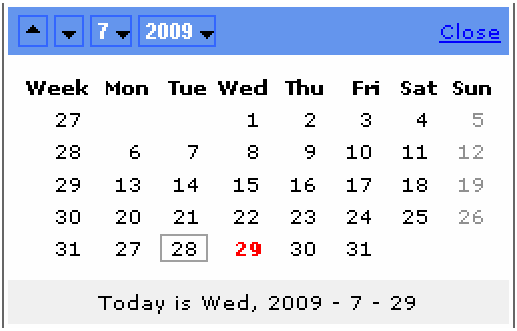
| | Department Name | ID Number | Name | Card | Group | Privilege |
|---|---|---|---|---|---|---|
| □ | | 1 | GgHhIiPp | 0 | Group1 | User |
| □ | | 4 | QqRrssTt | 0 | Group1 | User |
| □ | | 2 | UuVvJjKk | 0 | Group1 | User |
| □ | | 5 | LlAaBbCc | 0 | Group1 | User |
| □ | | 3 | MmNnOoWw | 0 | Group1 | User |
| □ | | 6 | nNOoDdEe | 0 | Group1 | User |
| □ | | 7 | [illegible] | 0 | Group1 | User |
| □ | | 8 | [illegible] | 0 | Group1 | User |
| □ | | 13 | EeFf | 0 | Group1 | User |
| □ | | 10 | 00010 | 0 | Group1 | User |
| □ | | 12 | IiHhGg | 0 | Group1 | User |
| □ | | 14 | 00014 | 0 | Group1 | User |
| □ | | 15 | 00015 | 0 | Group1 | User |
| □ | | 17 | 00017 | 0 | Group1 | User |
| □ | | 18 | 00018 | 0 | Group1 | User |

2. Input the date range of report

   1) Lay out period' s drop-down list, and select the date range.



2) If you want to self-define the date range, select the Date. Input the date range by selecting in the selection area of time zone.

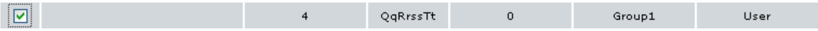


| Week | Mon | Tue | Wed | Thu | Fri | Sat | Sun |
|---|---|---|---|---|---|---|---|
| 27 | | | 1 | 2 | 3 | 4 | 5 |
| 28 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 29 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| 30 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |
| 31 | 27 | 28 | 29 | 30 | 31 | | |

Today is Wed, 2009 - 7 - 29

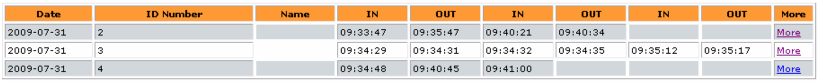
3. Specify the personnel to be queried

Tick the check box in the front of the personnel list.



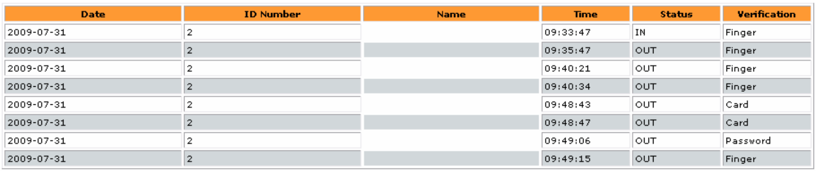
| | | | | | | |
|---|---|---|---|---|---|---|
| ☑ | | 4 | QqRrssTt | 0 | Group1 | User |

4. Click ‘Search’ to display the in&out records according with conditions on the new page.



| Date | ID Number | Name | IN | OUT | IN | OUT | IN | OUT | More |
|---|---|---|---|---|---|---|---|---|---|
| 2009-07-31 | 2 | | 09:33:47 | 09:35:47 | 09:40:21 | 09:40:34 | | | More |
| 2009-07-31 | 3 | | 09:34:29 | 09:34:31 | 09:34:32 | 09:34:35 | 09:35:12 | 09:35:17 | More |
| 2009-07-31 | 4 | | 09:34:48 | 09:40:45 | 09:41:00 | | | | More |

If you want to view more details, click the right “More” to display more in new page:



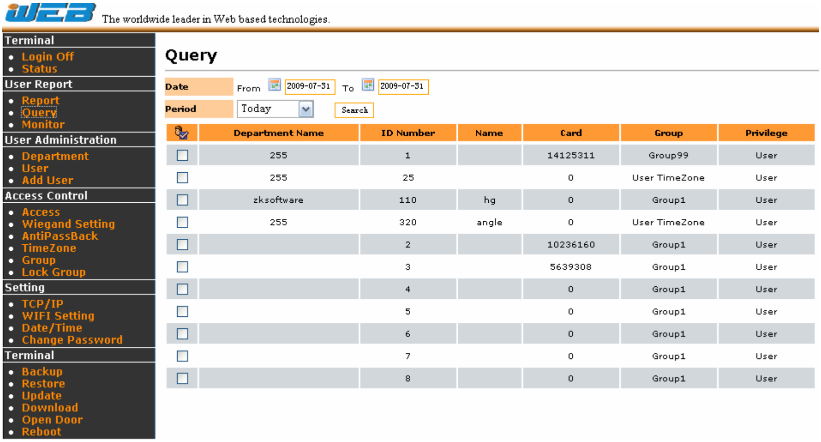
| Date | ID Number | Name | Time | Status | Verification |
|---|---|---|---|---|---|
| 2009-07-31 | 2 |  | 09:33:47 | IN | Finger |
| 2009-07-31 | 2 |  | 09:35:47 | OUT | Finger |
| 2009-07-31 | 2 |  | 09:40:21 | OUT | Finger |
| 2009-07-31 | 2 |  | 09:40:34 | OUT | Finger |
| 2009-07-31 | 2 |  | 09:48:43 | OUT | Card |
| 2009-07-31 | 2 |  | 09:48:47 | OUT | Card |
| 2009-07-31 | 2 |  | 09:49:06 | OUT | Password |
| 2009-07-31 | 2 |  | 09:49:15 | OUT | Finger |

## 3.2 Query records

**[function introduction]** Query all in-out records of specified personnel.

**[operating steps]**

1. Click "User report' → "Query" to open the Query window;



Query

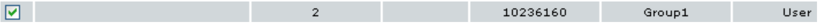
Date From 2009-07-31 To 2009-07-31

Period Today

|  | Department Name | ID Number | Name | Card | Group | Privilege |
|---|---|---|---|---|---|---|
| □ | 255 | 1 |  | 14125311 | Group99 | User |
| □ | 255 | 25 |  | 0 | User TimeZone | User |
| □ | zksoftware | 110 | hg | 0 | Group1 | User |
| □ | 255 | 320 | angle | 0 | User TimeZone | User |
| □ |  | 2 |  | 10236160 | Group1 | User |
| □ |  | 3 |  | 5639308 | Group1 | User |
| □ |  | 4 |  | 0 | Group1 | User |
| □ |  | 5 |  | 0 | Group1 | User |
| □ |  | 6 |  | 0 | Group1 | User |
| □ |  | 7 |  | 0 | Group1 | User |
| □ |  | 8 |  | 0 | Group1 | User |

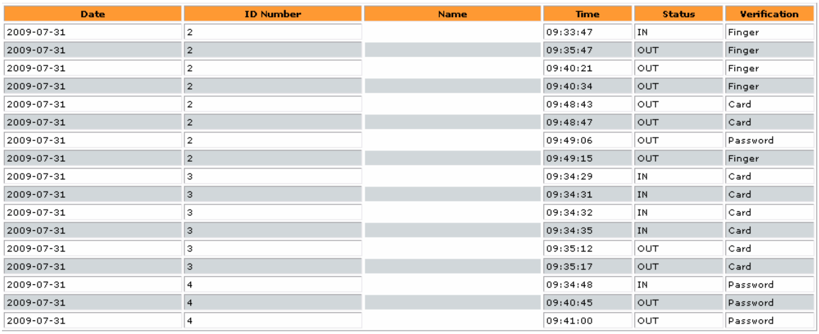
2. Specify the personnel to be queried

   1) Tick the check box in the front of personnel list.



|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
| ☑ |  | 2 |  | 10236160 | Group1 | User |

3. Click 'Search' to display the in-out records according with conditions on the new page.



| Date | ID Number | Name | Time | Status | Verification |
|---|---|---|---|---|---|
| 2009-07-31 | 2 |  | 09:33:47 | IN | Finger |
| 2009-07-31 | 2 |  | 09:35:47 | OUT | Finger |
| 2009-07-31 | 2 |  | 09:40:21 | OUT | Finger |
| 2009-07-31 | 2 |  | 09:40:34 | OUT | Finger |
| 2009-07-31 | 2 |  | 09:48:43 | OUT | Card |
| 2009-07-31 | 2 |  | 09:48:47 | OUT | Card |
| 2009-07-31 | 2 |  | 09:49:06 | OUT | Password |
| 2009-07-31 | 2 |  | 09:49:15 | OUT | Finger |
| 2009-07-31 | 3 |  | 09:34:29 | IN | Card |
| 2009-07-31 | 3 |  | 09:34:31 | IN | Card |
| 2009-07-31 | 3 |  | 09:34:32 | IN | Card |
| 2009-07-31 | 3 |  | 09:34:35 | IN | Card |
| 2009-07-31 | 3 |  | 09:35:12 | OUT | Card |
| 2009-07-31 | 3 |  | 09:35:17 | OUT | Card |
| 2009-07-31 | 4 |  | 09:34:48 | IN | Password |
| 2009-07-31 | 4 |  | 09:40:45 | OUT | Password |
| 2009-07-31 | 4 |  | 09:41:00 | OUT | Password |

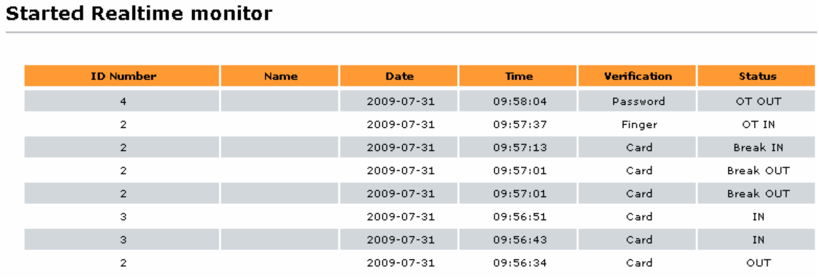
## 3.3 Realtime monitor

**[function introduction]** Realtime monitor all in-out records of current device.

**[operating steps]**

1. Click “User report” → “Monitor”, and enter into the monitor page;

2. System will display the got realtime records on the screen.



**Started Realtime monitor**

| ID Number | Name | Date | Time | Verification | Status |
|---|---|---|---|---|---|
| 4 |  | 2009-07-31 | 09:58:04 | Password | OT OUT |
| 2 |  | 2009-07-31 | 09:57:37 | Finger | OT IN |
| 2 |  | 2009-07-31 | 09:57:13 | Card | Break IN |
| 2 |  | 2009-07-31 | 09:57:01 | Card | Break OUT |
| 2 |  | 2009-07-31 | 09:57:01 | Card | Break OUT |
| 3 |  | 2009-07-31 | 09:56:51 | Card | IN |
| 3 |  | 2009-07-31 | 09:56:43 | Card | IN |
| 2 |  | 2009-07-31 | 09:56:34 | Card | OUT |

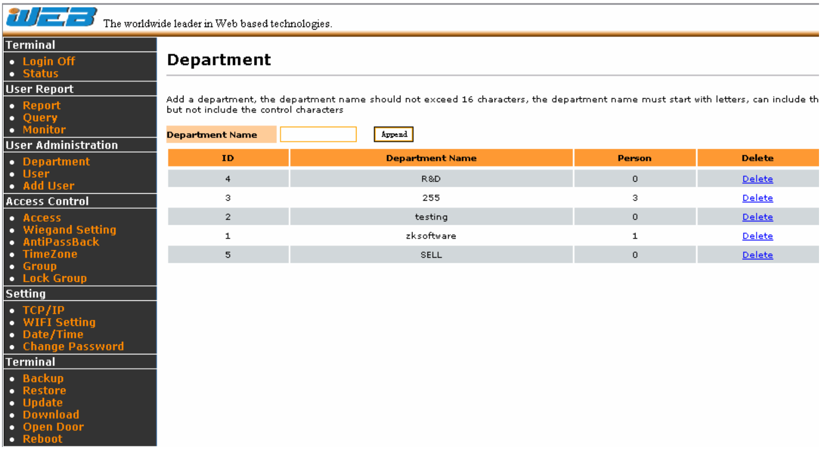
# 4. User Administration

## 4.1 Department management

**[function introduction]**Query, modify and delete the department that has existed in the system.

**[operating steps]**

1. Click "User Administration"→ "Department" to display the department information in the right page.



Department

Add a department, the department name should not exceed 16 characters, the department name must start with letters, can include th but not include the control characters

Department Name

| ID | Department Name | Person | Delete |
|---|---|---|---|
| 4 | R&D | 0 | Delete |
| 3 | 255 | 3 | Delete |
| 2 | testing | 0 | Delete |
| 1 | zksoftware | 1 | Delete |
| 5 | SELL | 0 | Delete |

2. Add a department

   1) Input the new department name in the textbox of Department Name.

   2) After inputting, click "Add" button, the new added department is displayed in the list.

3. Delete a department

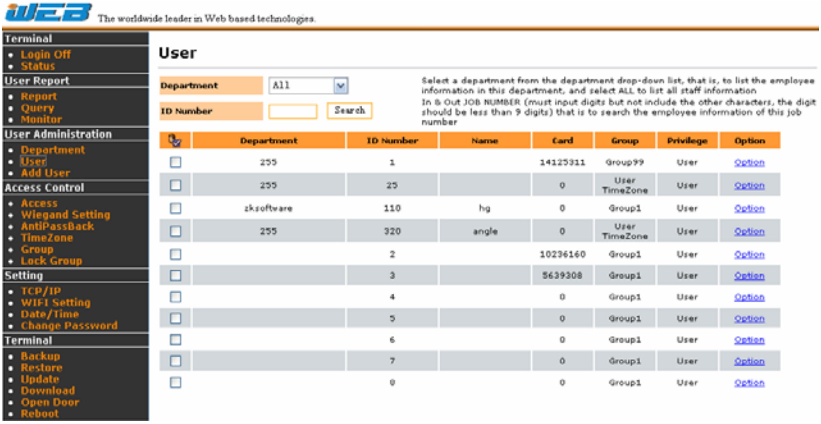
1) Click the ‘Delete’ button in the same line with the department that you want to delete, then the department is deleted from the system.

## 4.2 User Management

**[function introduction]** Query, modify and delete the personnel that have existed in the system.

**[operating steps]**

1. Click “User Administrator”→ “User” to display all staff information in the page;



User

Department: All

ID Number: Search

Select a department from the department drop-down list, that is, to list the employee information in this department, and select ALL to list all staff information

In & Out JOB NUMBER (must input digits but not include the other characters, the digit should be less than 9 digits) that is to search the employee information of this job number

| | Department | ID Number | Name | Card | Group | Privilege | Option |
|---|---|---|---|---|---|---|---|
| □ | 255 | 1 | | 14125311 | Group99 | User | Option |
| □ | 255 | 25 | | 0 | User TimeZone | User | Option |
| □ | zksoftware | 110 | hg | 0 | Group1 | User | Option |
| □ | 255 | 320 | angle | 0 | User TimeZone | User | Option |
| □ | | 2 | | 10236160 | Group1 | User | Option |
| □ | | 3 | | 5639308 | Group1 | User | Option |
| □ | | 4 | | 0 | Group1 | User | Option |
| □ | | 5 | | 0 | Group1 | User | Option |
| □ | | 6 | | 0 | Group1 | User | Option |
| □ | | 7 | | 0 | Group1 | User | Option |
| □ | | 8 | | 0 | Group1 | User | Option |

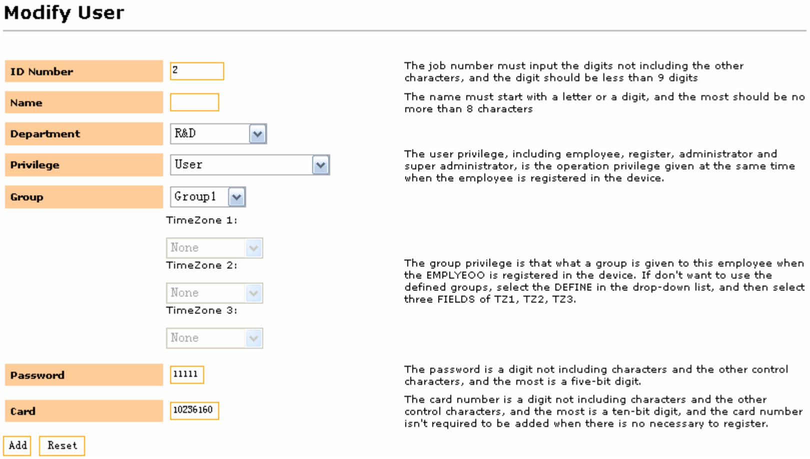
2. Query personnel

1) Select the department, which the personnel is belong to, in the drop-down department list.

2) Input the ID in ID number column and click “Search” button, then the personnel according with conditions will be displayed in the list.

3. Modify personnel's information

1) Click ‘Modification’ on the line where the personnel is to enter editing interface.



**Modify User**

|  |  |  |
|---|---|---|
| ID Number | 2 | The job number must input the digits not including the other characters, and the digit should be less than 9 digits |
| Name |  | The name must start with a letter or a digit, and the most should be no more than 8 characters |
| Department | R&D |  |
| Privilege | User | The user privilege, including employee, register, administrator and super administrator, is the operation privilege given at the same time when the employee is registered in the device. |
| Group | Group1<br>TimeZone 1: None<br>TimeZone 2: None<br>TimeZone 3: None | The group privilege is that what a group is given to this employee when the EMPLYEOO is registered in the device. If don't want to use the defined groups, select the DEFINE in the drop-down list, and then select three FIELDS of TZ1, TZ2, TZ3. |
| Password | 11111 | The password is a digit not including characters and the other control characters, and the most is a five-bit digit. |
| Card | 10236160 | The card number is a digit not including characters and the other control characters, and the most is a ten-bit digit, and the card number isn't required to be added when there is no necessary to register. |

**Remark:** If there is no access control function in device, items of group, privilege and so on will hide automatically.

2) In editing interface, the ID number can only be digits and can not be the same with the other ID and the ID range is in 1-9 bits. Except for ID, the other operations are the same as those of “Add User”.

3) During modifying, click the “Reset” button in the left-down corner to restore to the original information, or click “Add” button to return to the User page, then the modified personnel information is displayed in the list.

4. Delete the personnel's information

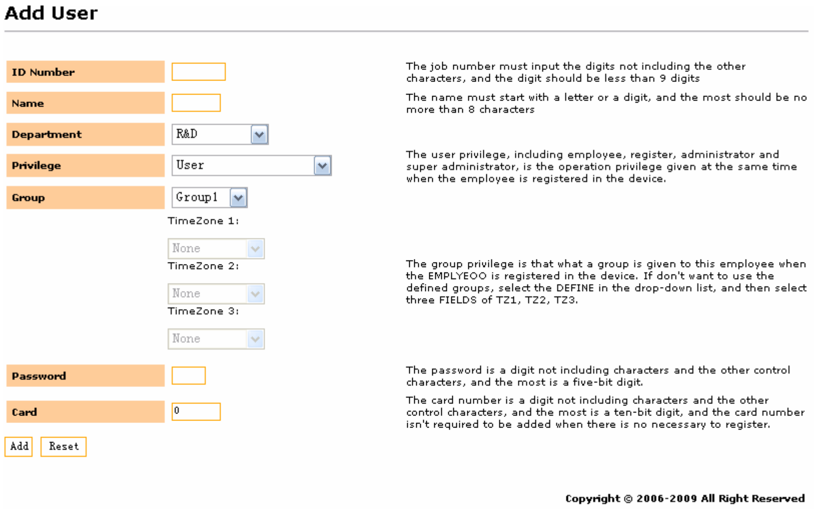
Click ‘Delete’ on the line where the personnel is to delete his information from the system.

## 4.3 Add User

**[function introduction]**Add a new employee to the system, and specify his access control privilege.

**[operating steps]**

1.Click “User administrator”→ “Add user”;



Add User

| | | |
|---|---|---|
| ID Number | | The job number must input the digits not including the other characters, and the digit should be less than 9 digits |
| Name | | The name must start with a letter or a digit, and the most should be no more than 8 characters |
| Department | R&D | |
| Privilege | User | The user privilege, including employee, register, administrator and super administrator, is the operation privilege given at the same time when the employee is registered in the device. |
| Group | Group1<br>TimeZone 1: None<br>TimeZone 2: None<br>TimeZone 3: None | The group privilege is that what a group is given to this employee when the EMPLYEOO is registered in the device. If don't want to use the defined groups, select the DEFINE in the drop-down list, and then select three FIELDS of TZ1, TZ2, TZ3. |
| Password | | The password is a digit not including characters and the other control characters, and the most is a five-bit digit. |
| Card | 0 | The card number is a digit not including characters and the other control characters, and the most is a ten-bit digit, and the card number isn't required to be added when there is no necessary to register. |

Copyright © 2006-2009 All Right Reserved

**Remark:** If there is no access control function in device, items of group, privilege and so on will hide automatically.

2. Input new user's information according to the page clues.

   1) Don’ t make the work number in collision (the work number is the digit from 1bit to 9 bits). Input the personnel’ s name (8 characters or 4 Chinese characters at most)

   2) Select user privilege (privilege for user to operate device).

   3) Select well-defined group in access control setting (group 1 by default).

If select the corresponding group number, then the user will use the set time zone of this group by default.

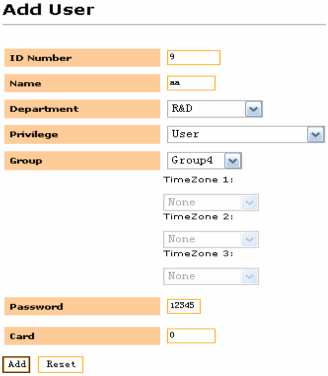
If not using group is selected, then another 3 time zones ('or' is among them) will be selected. Only in these 3 time zones, can the user have access control privilege.

4) The personnel who use password or card can input these two items.

5) Click “Add” after information filling is complete.

3. For example

1) User uses group time zone

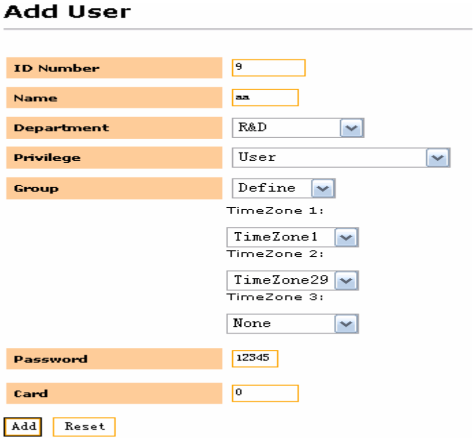


Add User

| | |
|---|---|
| ID Number | 9 |
| Name | aa |
| Department | R&D |
| Privilege | User |
| Group | Group4 |
| | TimeZone 1: None |
| | TimeZone 2: None |
| | TimeZone 3: None |
| Password | 12345 |
| Card | 0 |

The above setting shows: No. 9 personnel “aa” belongs to group 2 and use the time zone of Group4.

2) User does not use group time zone.

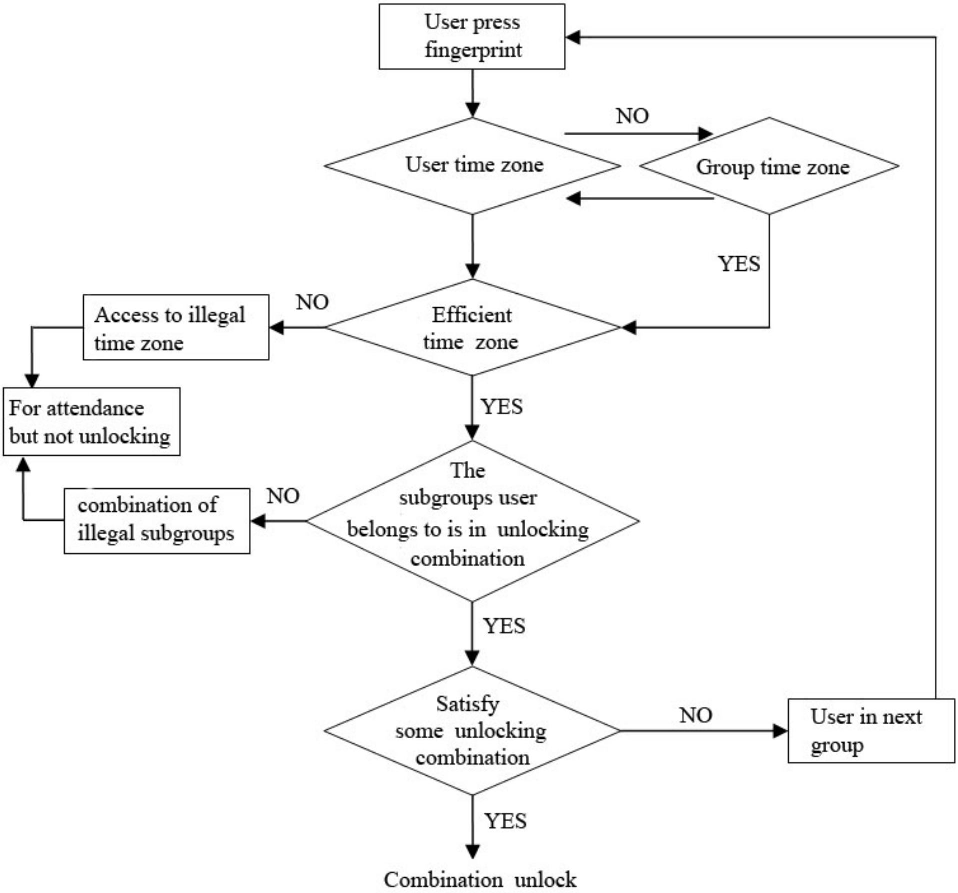


Add User

| | |
|---|---|
| ID Number | 9 |
| Name | aa |
| Department | R&D |
| Privilege | User |
| Group | Define<br>TimeZone 1:<br>TimeZone1<br>TimeZone 2:<br>TimeZone29<br>TimeZone 3:<br>None |
| Password | 12345 |
| Card | 0 |

The above setting shows: No. 9 personnel “aa” does not use group. He uses individual access control time zones, namely time zone 1 and time zone 29.

# 5. Access parameter setting



User press fingerprint
NO
User time zone
Group time zone
YES
NO
Access to illegal time zone
Efficient time zone
For attendance but not unlocking
YES
The subgroups user belongs to is in unlocking combination
NO
combination of illegal subgroups
YES
Satisfy some unlocking combination
NO
User in next group
YES
Combination unlock

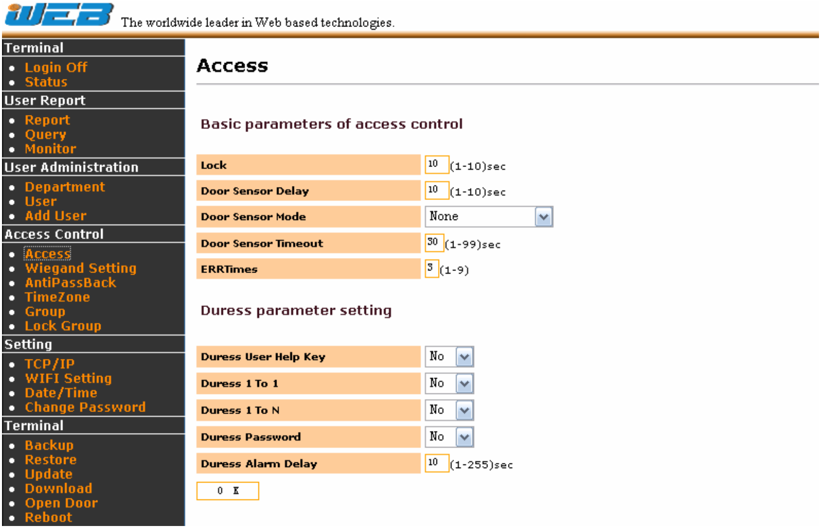
**Remark:** Only the device with access control function has this function.

## 5.1 Access Parameter Setting

**[function introduction]** the basic parameter settings and the advanced parameter settings of access control

**[operating steps]**

1. Click “Access control” → “Access”;



Access

Basic parameters of access control

| | | |
|---|---|---|
| Lock | 10 | (1-10)sec |
| Door Sensor Delay | 10 | (1-10)sec |
| Door Sensor Mode | None | |
| Door Sensor Timeout | 30 | (1-99)sec |
| ERRTimes | 3 | (1-9) |

Duress parameter setting

| | | |
|---|---|---|
| Duress User Help Key | No | |
| Duress 1 To 1 | No | |
| Duress 1 To N | No | |
| Duress Password | No | |
| Duress Alarm Delay | 10 | (1-255)sec |

2. According to the requirements to set parameters

1) Basic parameters setting

**Lock:** the time used to control unlocking. The minimum unit is 20ms, and the default is 100ms.

**Door Sensor Delay:** before starting alarm, there is a period of time after door opens, and this period of time is the door sensor delay.

**Door Sensor Mode:** normally open, normally close and none.

**Error Times:** when the number of unverified times is beyond the setting value, the system will generate a alarm signal.

2) Duress parameters setting: user can specify an enrolled fingerprint in the system as a duress fingerprint. In any case, this fingerprint identification will generate a duress alarm.

**Duress alarm delay:** after the duress alarm signal is generated, you can define a period of time (0-255 seconds) before outputting the alarm signal directly. The default value is 10.

**Alarm mode:** 1:1、 1:N and password. User can select one or several.

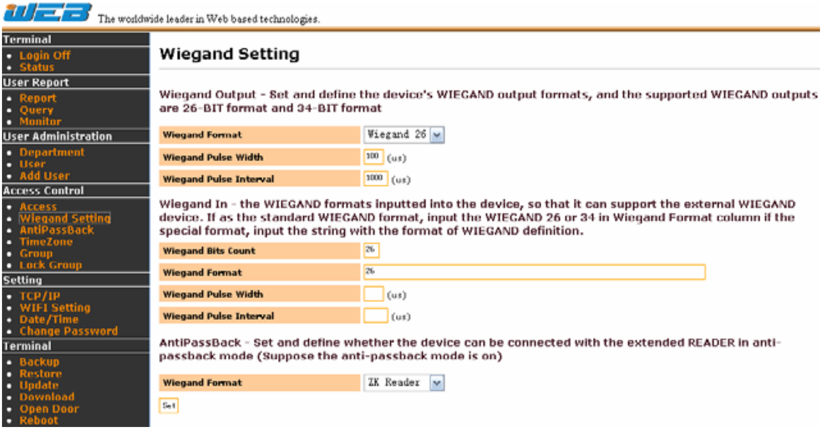
3. After setting, click “OK”，then restart the device to make the settings take effect.

## 5.2 Weigand Setting

**[function introduction]** Weigand out, Weigand in, as well as the reader selection under the format of the anti-passback Weigand.

**[operation steps]**

1. Click “Access Control” → “Wiegand Setting”;



Wiegand Setting

Wiegand Output - Set and define the device's WIEGAND output formats, and the supported WIEGAND outputs are 26-BIT format and 34-BIT format

| | |
|---|---|
| Wiegand Format | Wiegand 26 |
| Wiegand Pulse Width | 100 (us) |
| Wiegand Pulse Interval | 1000 (us) |

Wiegand In - the WIEGAND formats inputted into the device, so that it can support the external WIEGAND device. If as the standard WIEGAND format, input the WIEGAND 26 or 34 in Wiegand Format column if the special format, input the string with the format of WIEGAND definition.

| | |
|---|---|
| Wiegand Bits Count | 26 |
| Wiegand Format | 26 |
| Wiegand Pulse Width | (us) |
| Wiegand Pulse Interval | (us) |

AntiPassBack - Set and define whether the device can be connected with the extended READER in anti-passback mode (Suppose the anti-passback mode is on)

| | |
|---|---|
| Wiegand Format | ZK Reader |

2. According to requirements to set parameters

1) Wiegand out settings:

**Wiegand Format:** since the well-defined formats built in the system, don’t need users to designate the total bit length as well as each information’s location. Two formats of Wiegand 26 and Wiegand34, you can select from the drop-down list.

**Wiegnd Pulse Width:** the default pulse width sent by the Wiegand is 100 µs, but if the controller can not receive Wiegand, please adjust among the range from 1 to 999.

**Wiegand Pulse Interval:** the default value is 900, and the adjustable range is from 1 to 999.

2) Wiegand in settings:

**Wiegand Bits Count:** the output length of current format

**Wiegand Format:** the user defined Wiegand in format, if user selects the standard Wiegand 26 or Wiegand 34, needs not to input the format string, if other formats, user needs to list the corresponding format string.

**Wiegand Pulse Width:** the default pulse width sent by the Wiegand is 100μs, but if the controller can not receive the Wiegand, the adjustable range is from 1 to 999.

**Wiegand Pulse Interval:** the default value is 900, and the adjustable range is from 1 to 999.

3) The reader selection of anti-passback Wiegand

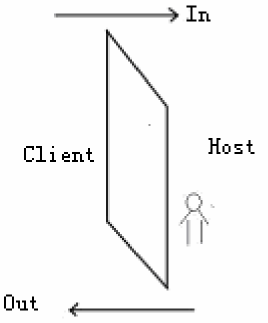
**Wiegand Format:** select the external reader supported by device in the case that the status of anti-passback is on.

3. After setting, click “Set” in the bottom left corner, then restart the device to make the settings take effect.

## 5.3 Anti-passback setting

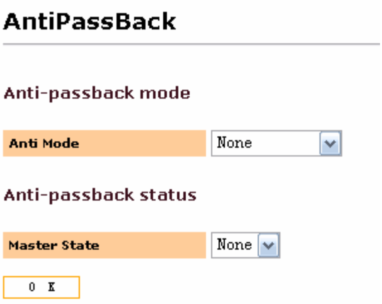
**[function introduction]** In order to prevent someone enters into the door but doesn’t go out by following the other person, you can use this function to avoid the safety hazard. The door can not be opened unless the out&in records are matched.

This function needs two machines to cooperate and realize. One machine is installed indoors (called as “Host” in the followings), and the other machine is installed outdoors (called as “Client” in the followings). Two machines can communicate through Wiegand signal.



**[operating steps]**

1. Click “Access Control” → “Antipassback”;



AntiPassBack

Anti-passback mode

Anti Mode: None

Anti-passback status

Master State: None

2. The selections of anti-pass back mode. There are 4 selections: out antipassback, in antipassback, in&out antipassback, no antipassback, none and save.

**Out anti-passback:** only the last record of user is the in record, does the door open. The first verification is able to open the door.

**In anti-passback:** only the last record of user is the out record, does the door open. The first verification is able to open the door.

**Out&in anti-passback:** only the out&in records are in accordance, does the door open. The first verification is able to open the door.

**None and save:** only the verification is passed between host and

Client, does the door open. No antipassback but reserve the status.

3. Master State

Three selections: control in, control out, none.

**Control in:** when set as this value, the records verified in this machine are the in records.

**Control out:** when set as this value, the records verified in this machine are the out records.

**None:** when set as this value, that is to close the anti-passback function in this machine.

4. After setting, click the down-left “OK” button, then restart the device to make the settings take effect.

## 5.4 Time Zone

**[function introduction]**Add and modify access control time zone which may be used by personnel.

Time zone is the smallest time zone unit of access control setting. The whole system can define 50 time zones at most. Every time zone defines seven time intervals, namely a week. Every interval is the efficient time zone in 24 hours every day. Every user can set 3 time zones at most. “or” exists in the three time zones. It is efficient only if verification time can satisfy one of them. The format of every time interval in time zone is HH:MM-HH:MM. That is, it is exact to minute.

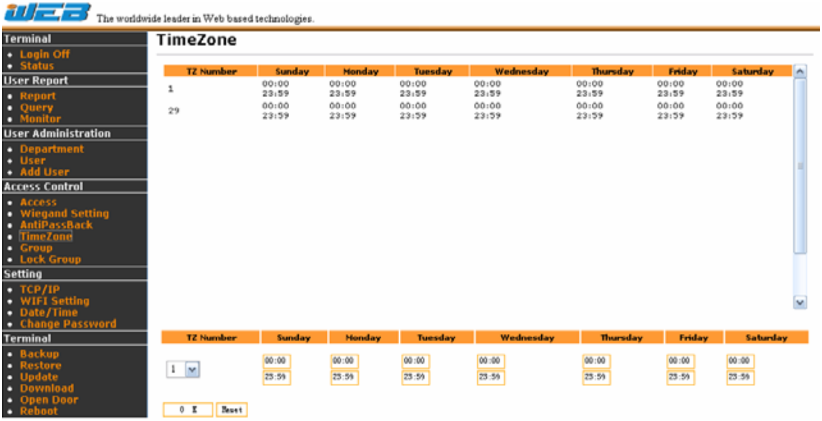
It means whole day forbidden if end time is smaller than start time （23:57- 23:56）. And it means that the interval is efficient is end time is bigger than start time （00:00- 23:59）.

Efficient time zone for user unlocking: whole day open （00：

00-23：59）or end time is bigger than start time.

**[operating steps]**

1.Click "Access Control"→"Time Zone";



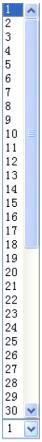
TimeZone

| TZ Number | Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday |
|---|---|---|---|---|---|---|---|
| 1 | 00:00<br>23:59 | 00:00<br>23:59 | 00:00<br>23:59 | 00:00<br>23:59 | 00:00<br>23:59 | 00:00<br>23:59 | 00:00<br>23:59 |
| 29 | 00:00<br>23:59 | 00:00<br>23:59 | 00:00<br>23:59 | 00:00<br>23:59 | 00:00<br>23:59 | 00:00<br>23:59 | 00:00<br>23:59 |

| TZ Number | Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday |
|---|---|---|---|---|---|---|---|
| 1 | 00:00<br>23:59 | 00:00<br>23:59 | 00:00<br>23:59 | 00:00<br>23:59 | 00:00<br>23:59 | 00:00<br>23:59 | 00:00<br>23:59 |

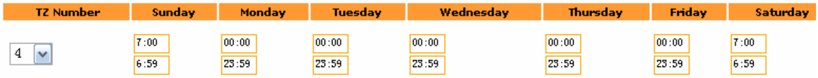
2. Add time zone

1) Lay out dropdown list of time zone number, and select the time zone number which does not exist in the list.



The time zone (which can be selected from the system) number range is 1—50.

2) Input time range (in time zone) to open the door.



| TZ Number | Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday |
|---|---|---|---|---|---|---|---|
| 4 | 7:00<br>6:59 | 00:00<br>23:59 | 00:00<br>23:59 | 00:00<br>23:59 | 00:00<br>23:59 | 00:00<br>23:59 | 7:00<br>6:59 |

The above setting shows that the door can be open whole day from Monday to Friday, but open-door is forbidden on Saturday and Sunday.

3) After inputting time zone information, click "OK" to save time zone setting, and the new time zone will be seen in the list.

3. Edit time zone

1) Lay out dropdown list of time zone number, and then select time zone number that you want to edit.

2) Input new time range.

3) After inputting, click "OK" to save the setting.

## 5.5 Group

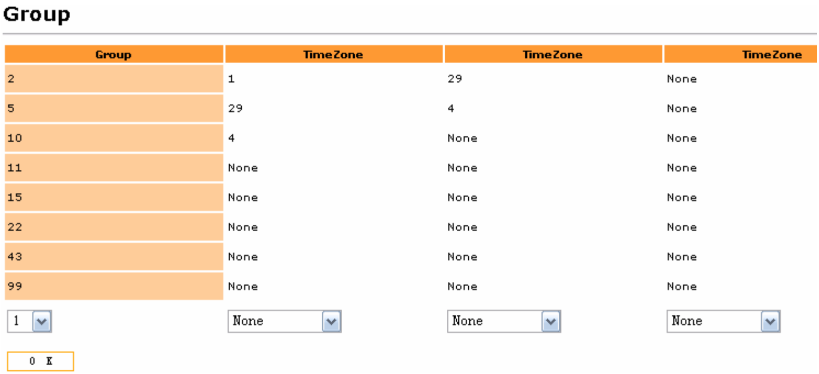
**[function introduction]**Set open-door time zone for 99 groups preset by the system.

Group setting can group users. 99 groups are defined by the system. The new enrolled user belongs to group 1 by default. He can also be reallocated to other groups through 'add user' or 'modify user information'. There are three time zones in group time zone, with 'or' existing among them.

**Notice:** In general, the device with black-white screen has defined 5 groups, and the device with color screen has defined 99 groups. They have the same functions. In this document, we set the color-screen device for example.

**[operating steps]**

1. Click "Access Control" → "Group";

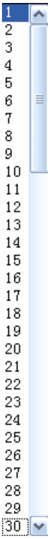


**Group**

| Group | TimeZone | TimeZone | TimeZone |
|---|---|---|---|
| 2 | 1 | 29 | None |
| 5 | 29 | 4 | None |
| 10 | 4 | None | None |
| 11 | None | None | None |
| 15 | None | None | None |
| 22 | None | None | None |
| 43 | None | None | None |
| 99 | None | None | None |
| 1 | None | None | None |

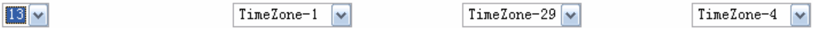
2. Add group setting

(1) Lay out dropdown list of time zone number, and select group number.



Group number which can be selected from the system ranges from 1 to 99.

(2) Input open-door time zone.



13 TimeZone-1 TimeZone-29 TimeZone-4

The above setting shows the open-door time zones for personnel in group 13 are time zone 1 & 29.

(3) Click “OK” to save the setting after input, and the new group setting will be seen in the list.

3. Edit group

1) Lay out dropdown list of time zone number, and select group number that you want to edit.

2) Input open-door time zone.

3) Click “OK” to save and cover the setting after input.

## 5.6 Lock Group

**[function introduction]** Set 10 unlocking combinations preset by the system.

Unlocking combination directly shows unlocking control. To prevent all enrolled users unlocking, make no settings for 10 unlocking combinations.

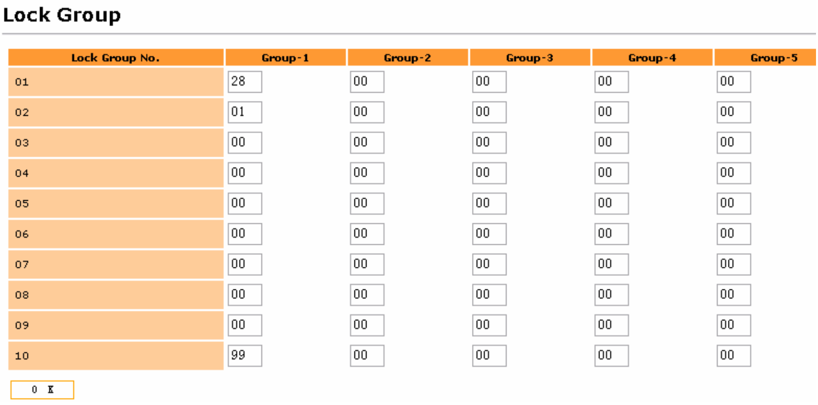
Unlocking combination setting is to define different unlocking combination. Every combination is made up of different groups. Unlocking combination directly use group number, without considering user verification order among various groups. For example: “123” means at least three users (one user respectively from group 1, group 2 and group 3 at least) can unlock after passing verification together. “4” shows that a single user in group 4 can unlock after passing verification.

The system can define 10 unlocking combination at most synchronously. Unlocking can be done only if user verification accords with one of them.

**Notice:** The system’s initial default unlocking combination is “1” (namely the new enrolled user can unlock by default).

**[operating steps]**

1. Click “Access Control” → “Lock Group”;

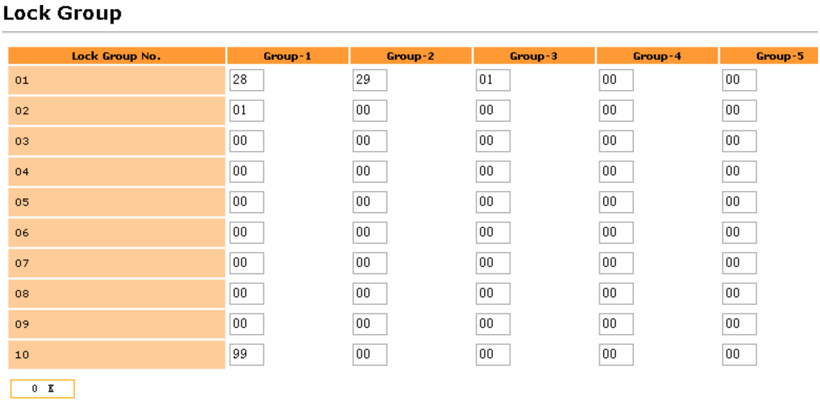


Lock Group

| Lock Group No. | Group-1 | Group-2 | Group-3 | Group-4 | Group-5 |
|---|---|---|---|---|---|
| 01 | 28 | 00 | 00 | 00 | 00 |
| 02 | 01 | 00 | 00 | 00 | 00 |
| 03 | 00 | 00 | 00 | 00 | 00 |
| 04 | 00 | 00 | 00 | 00 | 00 |
| 05 | 00 | 00 | 00 | 00 | 00 |
| 06 | 00 | 00 | 00 | 00 | 00 |
| 07 | 00 | 00 | 00 | 00 | 00 |
| 08 | 00 | 00 | 00 | 00 | 00 |
| 09 | 00 | 00 | 00 | 00 | 00 |
| 10 | 99 | 00 | 00 | 00 | 00 |

2. Unlocking combination setting

Tick the corresponding check box in the list to define the corresponding unlocking combination.



Lock Group

| Lock Group No. | Group-1 | Group-2 | Group-3 | Group-4 | Group-5 |
|---|---|---|---|---|---|
| 01 | 28 | 29 | 01 | 00 | 00 |
| 02 | 01 | 00 | 00 | 00 | 00 |
| 03 | 00 | 00 | 00 | 00 | 00 |
| 04 | 00 | 00 | 00 | 00 | 00 |
| 05 | 00 | 00 | 00 | 00 | 00 |
| 06 | 00 | 00 | 00 | 00 | 00 |
| 07 | 00 | 00 | 00 | 00 | 00 |
| 08 | 00 | 00 | 00 | 00 | 00 |
| 09 | 00 | 00 | 00 | 00 | 00 |
| 10 | 99 | 00 | 00 | 00 | 00 |

The above setting shows that 3 unlocking combinations are set. The group 1 is that unlocking can be done by successful verification of personnel in group 28, group 29, group 1. The group 2 is that unlocking can be only done by successful verification of personnel in group 1. The group 10 is that unlocking can be done by successful verification of personnel in the group 99.

**Notice:** the range of the unlocking combination is from 1 to 99.

3. Set unlocking combination, and click “OK” to save.

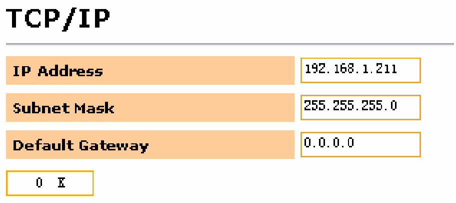
# 6. System Setting

## 6.1 TCP/IP Setting

**[function introduction]** Set the TCP/IP communication parameters, which are used in the communications between device and PC, by software settting.

**[operating steps]**

1. Click “Setting” → “TCP/IP”;



| | |
|---|---|
| IP Address | 192.168.1.211 |
| Subnet Mask | 255.255.255.0 |
| Default Gateway | 0.0.0.0 |

2. Input the device’s IP address, Subnet Mask, Default Gateway.

**IP address:** the default IP is 192.168.1.201, and you can modify according to the actual.

**Subnet Mask:** the default subnet mask is 255.255.255.0, and you can modify according to the actual.

**Default Gateway:** the default gateway is 0.0.0.0, and you can modify it according to the actual.

3. Click “OK” to write parameters into the device. The terminal device will restart automatically to make the changes take effect. If not restart, please restart the device by manual.

## 6.2 WIFI Setting

**[function introduction]** Set the WIFI parameters, which are used in wireless communications, by software setting.

Before the device is used in wireless device, as for 802.11 network, the other physical components such as access point, distribution system, wireless medium must exist. You must know the SSID (network identification name) used to access network.

**Network identification ID:** the network identification name used to access wireless network. (Distinguish the capital and small letter)

**Network mode:** here there are two modes, infrastructure model and Ad－hoc Model. The first corresponds to the star-structure network, and the second corresponds to the peer-to-peer network.

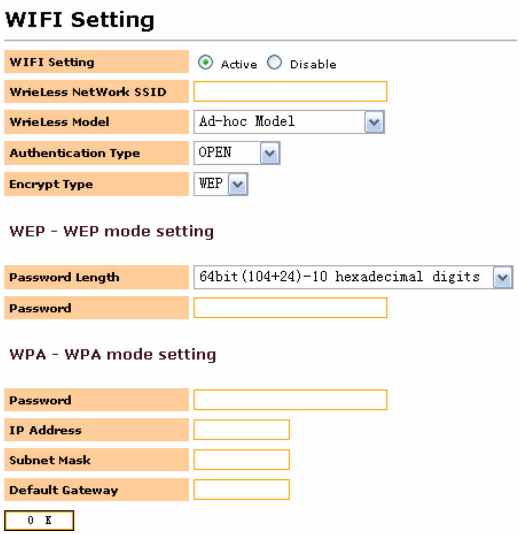
**Identification mode:** four modes of OPEN, SHARED, WEPAUTO, WPANONE are included by infrastructure model and Ad-hoc model.

**Encryption mode:** two modes of WEP (wired equivalent privacy) and WPA (WIFI protested access).

**This device's IP address:** If in 802.11 wireless network, has a function to distribute the address dynamically (DHCP). Otherwise, input the correct IP address, subnet mask etc. in the specified IP window.

**[operating steps]**

1. Click "Setting" → "WIFI Setting";



WIFI Setting

| | |
|---|---|
| WIFI Setting | ● Active ○ Disable |
| WrieLess NetWork SSID | |
| WrieLess Model | Ad-hoc Model |
| Authentication Type | OPEN |
| Encrypt Type | WEP |

WEP - WEP mode setting

| | |
|---|---|
| Password Length | 64bit(104+24)-10 hexadecimal digits |
| Password | |

WPA - WPA mode setting

| | |
|---|---|
| Password | |
| IP Address | |
| Subnet Mask | |
| Default Gateway | |

2. Activate WIFI, there are two items of “Activate” and “Disable” for selection. If select “Activate”, the wireless terminal will be activated, then you can configure the access point in 802.11 network. If select “Disable”, the wireless terminal will be disabled, then the user can set the way to connect the device and IP of wireless network.

3. Input the identification name of wireless network in the textbox of Wireless Network SSID, and select the corresponding parameters in the drop-down lists of wireless mode, authentication mode, and encrypt type.

4. Set passwords:

According to the authentication mode and encryption type, there are two ways of WEP and WPA to set passwords.

WEP password:

**Password length:** four options to select the password length

**Password:** input the password complying with the conditions.

**Notice:** If four passwords are set well in the WEP column, only the selected password is valid.

WPA password:

Input the password complying with the conditions.

5. The specified IP

Specify the IP of device in wireless network. No relation with the network setting in communication setting.

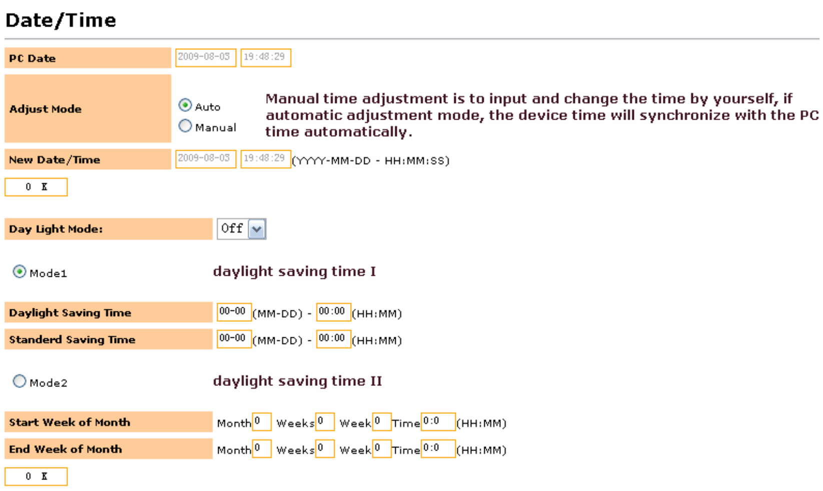
6. After setting, click “OK” button, then restart the device to make the settings take effect.

## 6.3 Time setting

**[function introduction]** Calibrate the device time and set the daylight saving time.

**[function introduction]**

1. Click “Setting” → “Date/Time”;



Date/Time

PC Date 2009-08-05 19:48:29

Adjust Mode ● Auto ○ Manual

Manual time adjustment is to input and change the time by yourself, if automatic adjustment mode, the device time will synchronize with the PC time automatically.

New Date/Time 2009-08-05 19:48:29 (YYYY-MM-DD - HH:MM:SS)

O K

Day Light Mode: Off

● Mode1 daylight saving time I

Daylight Saving Time 00-00 (MM-DD) - 00:00 (HH:MM)

Standerd Saving Time 00-00 (MM-DD) - 00:00 (HH:MM)

○ Mode2 daylight saving time II

Start Week of Month Month 0 Weeks 0 Week 0 Time 0:0 (HH:MM)

End Week of Month Month 0 Weeks 0 Week 0 Time 0:0 (HH:MM)

O K

2. Calibrate the device time

Two ways to calibrate: auto and manual. If select “Auto” in Adjust mode, the device time will synchronize with the PC time. If select “Manual”, the user will set the device time manually. In two textboxes of New Date/Time, input the new date and time. The date format is YYYY-MM-DD and the time format is HH:MM:SS. After setting, click “OK” in Date/Time.

**Note:** “PC Date” is only as a reference to calibrate time.

3. Set daylight saving time

In the drop-down list of Daylight Saving model, select “ON” to open the daylight saving time, or select “OFF” to close the daylight saving time.

If select “ON” in model, there are two models of daylight saving time: model1 and model2.

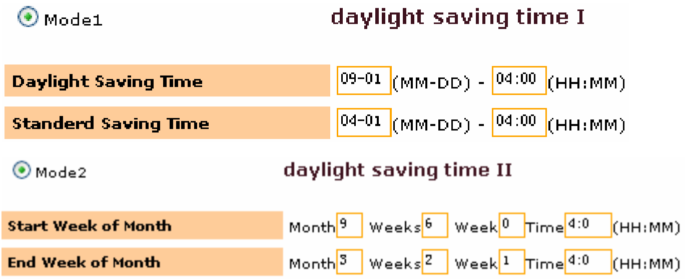
If select model1, it indicates to set the daylight saving time as MM-DD HH:MM format, and this model is the default model.

If select model2, it indicates to set the daylight saving time as MM WS WK HH:MM format.

The value range of WS is: 1-6, 1 indicates the first week and 2 indicates the second week, and so on. The value range of WK is: 0-6, 0 indicates Sunday and 1 indicates Monday, and so on.

For example:

We set an example as 2008-9-1 4:00 (Sunday, the first week, September 2008) to introduce the two modes:



● Mode1 daylight saving time I

| | | |
|---|---|---|
| Daylight Saving Time | 09-01 (MM-DD) - | 04:00 (HH:MM) |
| Standerd Saving Time | 04-01 (MM-DD) - | 04:00 (HH:MM) |

● Mode2 daylight saving time II

| | | | | |
|---|---|---|---|---|
| Start Week of Month | Month 9 | Weeks 6 | Week 0 | Time 4:0 (HH:MM) |
| End Week of Month | Month 3 | Weeks 2 | Week 1 | Time 4:0 (HH:MM) |

**Notice:**

1. If the start month of daylight saving time is bigger than the end time of daylight saving time, it indicates to straddle over year. For example: start 2007-9-1 4:000, end 2008-4-1 4:00.

2. If select model2, set the start time of daylight saving time: Sunday, the sixth week, September, 2007. Then in 2008, since no the sixth week but fifth week in September, system will regard the time of last Sunday of that month as the start time to enter into the daylight saving time.

3. If set the start time of daylight saving time as Monday, the first week, September, 2008. Then in 2009, since the first day of September is Tuesday not Monday, system will find the first Monday in that month automatically in this case.

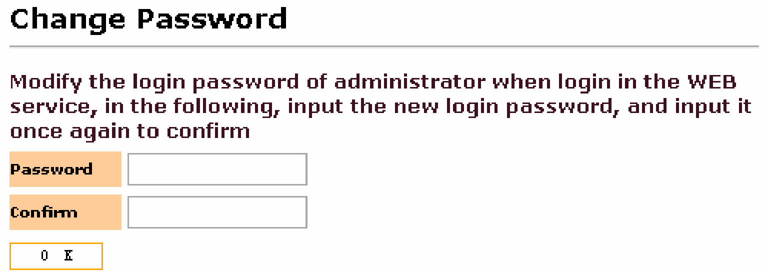
**Notice**: The color-screen device can only use model 1.

## 6.4 Password

**[function introduction]** Modify the administrator password used to login in Web server.

**[operating steps]**

1. Click “Setting” → “Password”;



Change Password

Modify the login password of administrator when login in the WEB service, in the following, input the new login password, and input it once again to confirm

2. Input new password twice, and click “OK” button.
3. After modifying, need to log off the system and log in again.

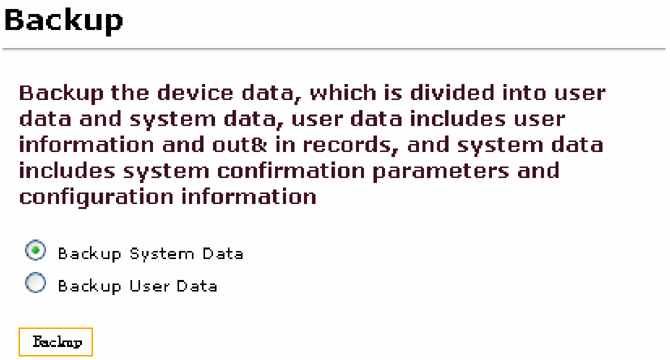
# 7. Terminal

## 7.1 Backup

**[function introduction]** Backup system data and user data, include configuration information of system parameters and user information as well as in&out records.

**[operating steps]**

1.Click “Terminal” → “Backup”;



Backup

Backup the device data, which is divided into user data and system data, user data includes user information and out& in records, and system data includes system confirmation parameters and configuration information

● Backup System Data

○ Backup User Data

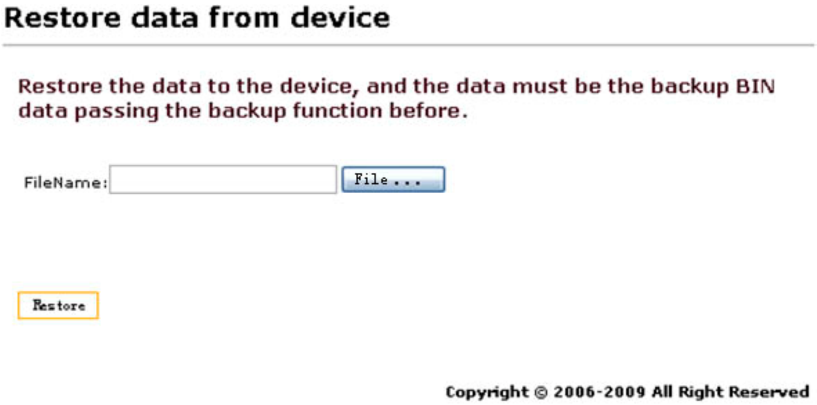
2. Select Backup System Data or Backup User data, click “Backup” button to pop up the message box. Save data to the designated path.

## 7.2 Restore

**[function introduction]** Restore data to the device, the data must be the previous BIN data backed up through the backup function.

**[operating steps]**

1. Click “Terminal” → “Restore”;



Restore data from device

Restore the data to the device, and the data must be the backup BIN data passing the backup function before.

FileName:

Copyright © 2006-2009 All Right Reserved

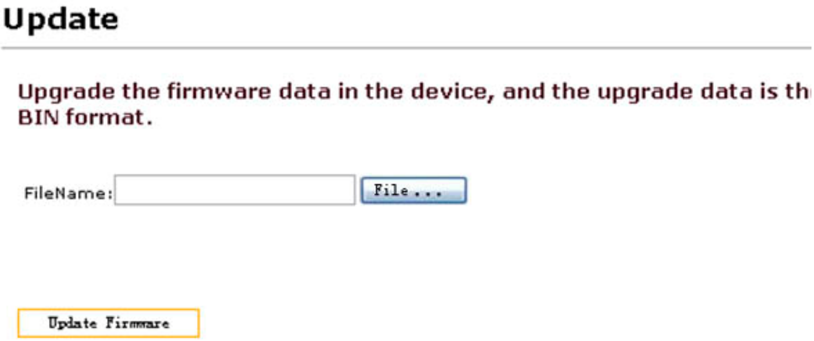
2. Click “Browse” button, then select the backup data saved in the local.
3. Click “Restore” button to restore data to the device.

### 7.3 Update

**[function introduction]** Update the firmware data in device, and update the data package as BIN format.

**[operating steps]**

1. Click “Terminal” → “Update”;



Update

Upgrade the firmware data in the device, and the upgrade data is th
BIN format.

2. Click “Browse” button, then select the firmware data saved in the local.

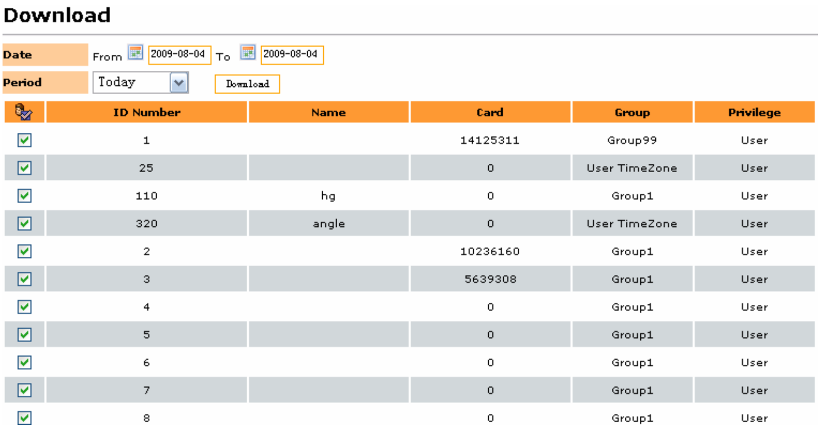
3. Click “Update Firmware” button to update the firmware of device.

### 7.4 Download

**[function introduction]** Modify the password of current user who has logged in.

**[operating steps]**

1. Click “Terminal” → “Download”;



Download

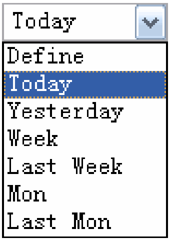
Date From 2009-08-04 To 2009-08-04

Period Today

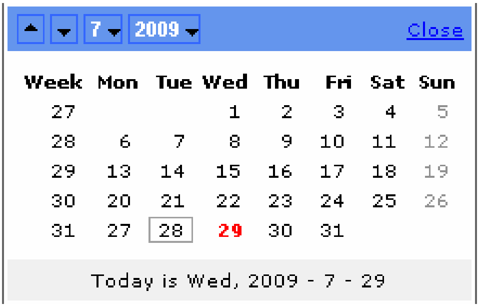
| | ID Number | Name | Card | Group | Privilege |
|---|---|---|---|---|---|
| ☑ | 1 | | 14125311 | Group99 | User |
| ☑ | 25 | | 0 | User TimeZone | User |
| ☑ | 110 | hg | 0 | Group1 | User |
| ☑ | 320 | angle | 0 | User TimeZone | User |
| ☑ | 2 | | 10236160 | Group1 | User |
| ☑ | 3 | | 5639308 | Group1 | User |
| ☑ | 4 | | 0 | Group1 | User |
| ☑ | 5 | | 0 | Group1 | User |
| ☑ | 6 | | 0 | Group1 | User |
| ☑ | 7 | | 0 | Group1 | User |
| ☑ | 8 | | 0 | Group1 | User |

2. Input the date range of downloading.

1) Pop up the drop-down list of period, and select the desired date range.



2) If you want to self-define the time range, select the Date. Input the date range by selecting the date in time selection area.

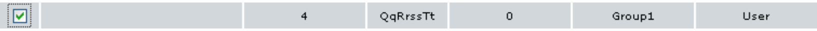


| Week | Mon | Tue | Wed | Thu | Fri | Sat | Sun |
|---|---|---|---|---|---|---|---|
| 27 |  |  | 1 | 2 | 3 | 4 | 5 |
| 28 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| 29 | 13 | 14 | 15 | 16 | 17 | 18 | 19 |
| 30 | 20 | 21 | 22 | 23 | 24 | 25 | 26 |
| 31 | 27 | 28 | 29 | 30 | 31 |  |  |

Today is Wed, 2009 - 7 - 29

3. Designated personnel

1) Tick the check box at the front in the personnel list.



|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
| ☑ |  | 4 | QqRrssTt | 0 | Group1 | User |

4. Click "Download" button to pop up the Save message box, after designating the path, download the in&out records complying with the conditions to the local PC.

## 7.5 Open Door

**[function introduction]** Modify the password of current user who has logged in.

**[operating steps]**

1. Click "Terminal" → "Open Door"

2. System informs "The door is open".

## 7.6 Reboot

**[function introduction]** Reboot the device remotely by Web server.

**[operating steps]**

1. Click “Terminal” → “Reboot”

2. System informs “Device is rebooting, please connect device later”.

# Appendix 1 how to connect a terminal unit to network

## 1. Terminal unit requirement

Web Server function, namely device’s selective function, needs firmware support of device.

☺Tip：Please consult technicians or contact business representatives of company if you need this function.

## 2. Terminal unit parameters

1）enter device’s menu—setting—communication setting to find the following items:

IP address
Network speed rate
Gateway address
Subnet mask

**IP address:** allocate IP address for the device.

**Network speed rate:** select corresponding network speed rate according to actual network environment.

If access needs crossing network segment, gateway address and subnet mask need to be set.

## 3. Set device’s parameters according to different network environment

1）If PC and terminal unit are in the same network segment of a LAN.

“IP address” and “network speed rate” need to be set.

For example: PC’s IP is 192.168.1.100, and device’s IP is 192.168.1.201.

When logging in Web server on PC, input 192.168.1.201 in browser’s address column.

2）If PC and terminal unit are in the same LAN, but in different network segment.

IP address, network speed rate, gateway and subnet mask need to be set.

3）If PC and terminal unit are not in the same LAN, terminal unit must possess a public network IP for PC to access.