PUSH SDK Communication Protocol

Version：Ver. 2.0.1

Date：2011.8

1 Preface

1.1 Objective

This document presents the prototype design requirements of customers and developers so as to guide the firmware and server development engineers through the software development.

1.2 Design Principle

This document helps development engineers optimize and add new features to the original PUSH SDK protocol and servers including the ADMS, Time8.0.

1.3 Terminology

Upload: Refers to the sending of data from the equipment to the server.

Download: Refers to the downloading of data from the server to the equipment.

2 General Design

2.1 System Structure

Servers: Support ADMS, Time8.0, and Att2008.

Software indexes:

- Support current mainstream firmware with black-and-white, 3.5-inch, 3-inch, or 8-inch screens.
- Provide standardized and optimized access interfaces on the server.
- Provide database access interfaces that adapt to different firmware.
- Support all time zones including half-hour time zones.
- Support automatic uploading of attendance records.
- Support automatic uploading of attendance photos.
- Support automatic uploading of system logs.
- Support automatic uploading of modified/added user information including basic user information, fingerprints, and images of faces and fingerprints.
- Support automatic deleting of oldest data (the amount of deleted data is configurable) when attendance records or photos overflow.
- Support receiving notification commands (UDP command notification requires network support) on the server.
- Support delivering system commands such as the **ls** command from the server.
- Support checking equipment data updating conditions from the server.

- Support purging attendance records, attendance photos, and user information from the equipment.
- Support acquiring basic equipment information.
- Support setting equipment items.
- Support restarting the equipment.
- Support reloading equipment items.
- Support equipment unlocking.
- Support canceling alarm generation of the equipment.
- Support detecting and sending new data.
- Support reading equipment files.
- Support downloading files from the server to the equipment (including firmware upgrading).
- Support downloading SMS messages from the server to the equipment.
- Support adding, modifying, or deleting user information and fingerprints of the equipment.
- Support registering user fingerprints (the facial recognition by machine is temporarily unavailable).
- Support domain name resolution.
- ***Support the equipment access authentication mechanism.***
- ***Support automatic correction of attendance data including attendance records and photos.***
- ***Support setting unlocking combination and time segment of the equipment.***
- ***Support downloading user photos from the server.***
- ***Support uploading attendance records or photos within a specified duration from the server.***
- ***Support querying basis user information exclusive of fingerprints and faces of the equipment.***
- ***Support HTTPS.***
- ***Support automatic uploading of fingerprint photos.***

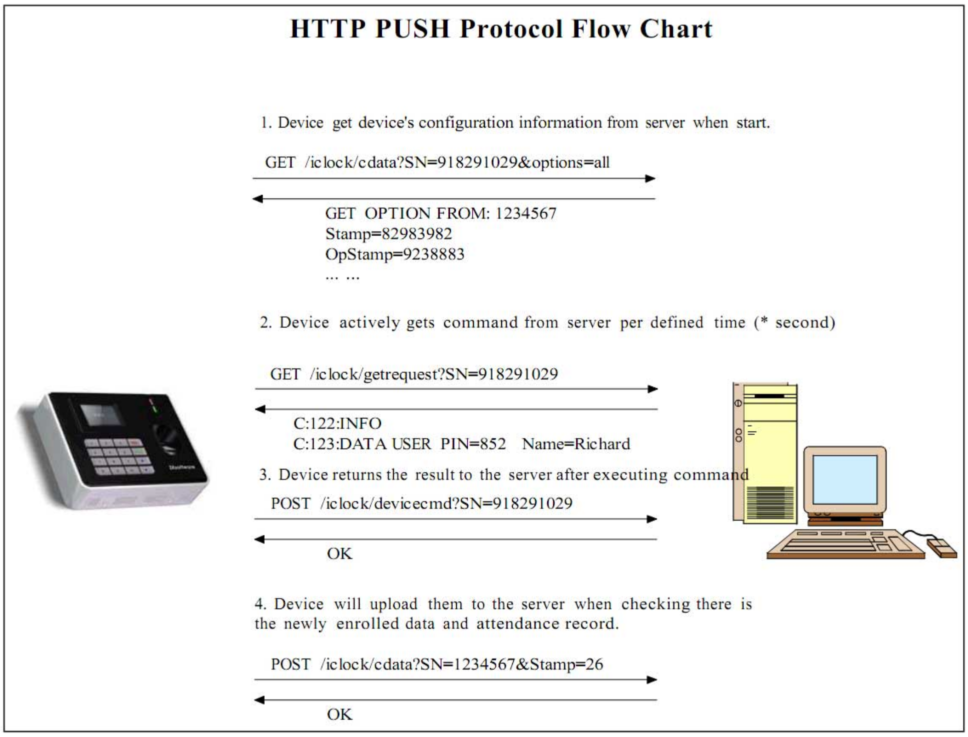
Note: 1. In this document, all functions shown in bold and fonts are to be implemented in successive releases.

2.2 Operating Environment

For details, see *Requirement Analysis Instructions*.

3 Function Details

3.1 PUSH SDK Protocol Flowchart



HTTP PUSH Protocol Flow Chart

1. Device get device's configuration information from server when start.

```
GET /iclock/cdata?SN=918291029&options=all
```

```
GET OPTION FROM: 1234567
Stamp=82983982
OpStamp=9238883
... ...
```

2. Device actively gets command from server per defined time (* second)

```
GET /iclock/getrequest?SN=918291029
```

```
C:122:INFO
C:123:DATA USER PIN=852   Name=Richard
```

3. Device returns the result to the server after executing command

```
POST /iclock/devicecmd?SN=918291029
```

```
OK
```

4. Device will upload them to the server when checking there is the newly enrolled data and attendance record.

```
POST /iclock/cdata?SN=1234567&Stamp=26
```

```
OK
```

3.2 PUSH SDK Communication Protocol

PUSH SDK is a ZTE-developed HTTP-based communication protocol and supports data transmission by allowing the equipment to actively connect to the server. Its major applicable environments are stable networks where the TCP or IP is supported, for example widely-used LAN and WWW.

Advantages:

(1) Update new data actively.

(2) Support resumable download.

(3) Facilitate function development or expansion.

Disadvantages: Only support the TCP/IP communication modes.

Note: Your selected model must support PUSH SDK functions.

LEVEL: WEB development engineers

1. Communication Between Equipment and Server

The equipment communicates with the server through the HTTP and additionally sends data to the server using **GET** or **POST** commands. The server then returns a result in response. All data except for specified file contents is transmitted in plain text. Text files are composed of lines separated by and ended with a line feed character "\n". If FieldName=Value is adopted during resolution of received texts, read the Value according to the FieldName. The FieldName field contained in a received text varies with different equipment functions. For example, the user information text received by a fingerprint-specified equipment does not contain any card information; otherwise, the text received by a equipment that supports RF card functions contains the card information, as shown below.

User information received by a equipment supports fingerprint verification only:

USER PIN=982 Name=Richard Passwd=9822 Grp=1 TZ=

User information received by a fingerprint equipment that supports RF card functions:

USER PIN=982 Name=Richard Passwd=9822 ***Card=[09E4812202]*** Grp=1 TZ=

Considering that the equipment judges whether the server properly responds and synchronizes with the equipment time according to the HTTP header, the server provides standard HTTP header information in returned data, for example:

```
HTTP/1.1 200 OK
Content-Type: text/plain
Date: Thu, 19 Feb 2008 15:52:10 GMT
```

C language formatting strings are commonly used for data formatting. All formulated formatting characters start with Character “%”. The following formats are used in this document:

%d: Indicates a decimal integer.

%s: Indicates a character string.

%x or %X: Indicates an unsigned integer in hexadecimal format.

The inserted digit between "%" and the regulated formatting character indicates the maximum field width. For example, %3d indicates a 3 decimal integer. If there are less than 3 digits, pad blank spaces to the leftmost side. %8s indicates an 8-character string. If there are less than 8 characters, pad blank spaces to the leftmost side. If the string length or number of integer digits exceeds the field width, export the string in accordance with its actual length. Furthermore, you can pad a string with zeros by adding a “0” before the field width item. For example, %04d indicates that when there are less than 4 digits, zeros are padded on the leftmost to make the result a four-digit string. The default padding place is on the left, but it can be on the right if you set the field width to a negative number.

2. Server Configuration Information Reading

The equipment must first read configuration information on the server, and then perform data communication with the server as required.

The equipment sends:

```
GET /iclock/cdata?SN=xxxxxx&options=all&pushver=2.0.1&language=XX
```

Where xxxxxx indicates the equipment serial number (SN). 2.0.1 indicates current PUSH SDK library protocol release. Older releases do not support the protocol version number. XX indicates the language ID. For details, see the firmware language ID description as follows:

Identifier	Description
s83	Chinese
69	English
…	…

The server returns (for example):

```
GET OPTION FROM: 123456
Stamp=82983982
OpStamp=9238883
PhotoStamp=9238833
ErrorDelay=60
Delay=30
TransTimes=00:00;14:05
TransInterval=1
TransFlag=1111000000
Realtime=1
Encrypt=0
ServerVer=3.4.1 2010-06-07
TableNameStamp=XXXXXX
```

Where:

GET OPTION FROM: Followed by the SN of the corresponding equipment.

Stamp: Followed by the latest record timestamp tag of attendance records last uploaded by the equipment. (This field is available for protocol firmware of previous versions but unavailable for those of updated versions.)

OpStamp: Followed by the latest operation record timestamp tag of personnel data last uploaded by the equipment. (This field is available for protocol firmware of previous versions but unavailable for those of updated versions.)

PhotoStamp: Followed by the record timestamp tag of onsite verification photos last uploaded by the equipment. (This field is available for protocol firmware of previous versions but unavailable for those of updated versions.)

ErrorDelay: Indicates the interval (unit: second) between attempts to reconnect to the server after a network connection failure occurs.

Delay: Indicates the interval (unit: second) between attempts to connect to the server in the event of proper network connection.

TransTimes: Indicates the time (time: minute in a 24-hour format) to regularly check and transfer data. A semicolon is used to separate a maximum amount of ten time settings.

TransInterval: Indicates the interval (unit: minute) during which new data is checked and transferred.

TransFlag: Specifies which data IDs are to be transferred from the equipment to the server.

Return “1111000000" or other similar character array IDs if protocol firmware of previous versions are adopted. Return ”0000000000” if previous Att2008 attendance software is adopted to upload attendance picture IDs only. New Att2008 requires you to set the attendance picture ID uploading. 0 indicates that this type of data is forbidden to be uploaded automatically. 1 Indicates that this type of data is allowed to be uploaded automatically. Table 2-1 lists the IDs of data types that can be automatically uploaded by current hardware in a standard configuration state.

Return “TransData AttLog\tOpLog\tAttPhoto” or other similar string IDs if current version of firmware is adopted. If you want to automatically upload data of a specified type, set relevant string IDs. Table 2-1 lists the IDs of data types that can be automatically uploaded by current hardware in a standard configuration state.

To automatically upload users and fingerprints, you must set automatic operation log uploading

Allowable Transmission Data Types		Description
String ID	Character Array ID	
AttLog	0	Indicates the attendance record.
OpLog	1	Indicates the operation log.
AttPhoto	2	Indicates the attendance photo.
EnrollUser	4	Enrolls a user.
ChgUser	6	Changes the user information.
EnrollFP	3	Enrolls a fingerprint.
ChgFP	7	Changes a fingerprint.
FPImag	5	Indicates the fingerprint image.

Table 2-1

Realtime: Indicates whether to realtime transfer new records. When Realtime=1, new data, if any, is transferred to the server. When Realtime=0, the data is transferred at the time specified by TransTimes and TransInterval.

Encrypt: Indicates whether to encrypt the transferred data (Granding-specified encryption algorithm is used for encrypted transfers). Return 0.

ServerVer: Indicates the server version and time (The time format is undetermined. The protocol firmware of previous versions supports this parameter).

TableNameStamp: Indicates automatically uploaded data timestamps. TableName corresponds to the name of a table and is consistent with the registered name of the firmware. Stamp is a fixed label. All timestamps of automatically uploaded data tables must be returned to the equipment. The timestamp of each data table occupies a line by adopting the following form:

TableNameStamp=XXXXX

For example, ATTLOGStamp=82983982 indicates the attendance record timestamp.

Table 2-2 lists the table names supported by the firmware in a standard configuration state (the table names must be capitalized).

Table Name	Function	Whether to support automatic uploading?
ATTLOG	Attendance record	Y
OPERLOG	Operation log	Y (including operation data of operation logs and records, for example modified users and registered fingerprints)
ATTPHOTO	Attendance photo	Y
SMS	SMS message	N
USER_SMS	List of individual SMS users	N
USERINFO	User information	N
FINGERTMP	Fingerprint template	N

Table 2-2

Relationship of TransTimes, TransInterval, and Realtime:

1) If Realtime is set to 1, immediately update the data regardless of whether the other two items are configured.

2) If TransInterval is larger than 0, upload the data at a specified time regardless of whether the other two items are configured.

3) If TransTimes specifies the time. This setting is of no use if other two items are configured with a valid value.

3. Data Updating

1. Upload the Attendance Record

The equipment sends:

```
POST /iclock/cdata?SN=xxxxxx&table= ATTLOG&Stamp=99999999
982 2008-02-25 12:08:21 1 0
982 2008-02-25 18:01:09 1 0
```

Where xxxxxx indicates the equipment SN. ATTLOG indicates the attendance record table name of current firmware (see Table 2-2) in a standard configuration state. 99999999 indicates the latest record timestamp of the data updated this time. The server records the timestamp to ATTLOGStamp (see Table 2-2) for this equipment to easily return from reading configuration information.

According to specific equipment configurations, a piece of record contains multiple fields separated with a tab \t. These fields include:

PIN——User attendance number

TIME——Attendance time

STATUS——Attendance status (see Table 2-3)

VERIFY——Verification mode (see Table 2-3)

WORKCODE——Work code

RESERVED1——Reserved 1

RESERVED2——Reserved 2

Some attendance machines do not have the last three fields.

Verification Mode	Attendance Status
0 ——Password 1 —— Fingerprint 2 —— Card 9 ——Others	0——Clock in 1—— Clock out 2—— Out 3—— Return from an out 4——Clock in for overtime 5—— Clock out for overtime 8——Meal start 9—— Meal end

Table 2-3

The server returns:

OK

If the server returns an error page (HTTP 404 or 500) or fails to respond for a long time (overtime), this equipment thinks that this data transfer fails and sends this data again.

2. Update the User Information and System Log

The equipment sends:

```
POST /iclock/cdata?SN=xxxxxx&table=OPERLOG&Stamp=99999999
USER PIN=982 Name=Richard Passwd=9822 Card=[09E4812202] Grp=1 TZ=
POST /iclock/cdata?SN=xxxxxx&table=OPERLOG&Stamp=99999999
```

```
FP PIN=982 FID=1 Valid=1 TMP=ocoRgZPRN8EwJNQxQTY......
```

Where xxxxxx indicates the equipment SN. OPERLOG indicates the operation log table name of current firmware (see Table 2-2) in a standard configuration state. 99999999 indicates the latest operation record timestamp of the data updated this time. The server records the timestamp to OPERLOGStamp (see Table 2-3) for this equipment to easily return from reading configuration information.

Each record begins with a start tag indicating contents of this record followed by a space and field values of this record, and ends with a line feed character "\n". Between those file characters are a tab \t. Each field is generally assigned a value by way of FieldName=Value. For details about specific formats and contents, see Table 2-4 and Table 2-5.

Start Tag	Record Content	Field Description

USER	Basic user information	PIN=982: Indicates the user attendance number.
		Name=Richard: Indicates the user name.
		Passwd=9822: Indicates the password.
		Card=[09E4812202]: Indicates the ID card number.
		Grp=1
		TZ=

FP	User fingerprint template	PIN=982: Indicates the user attendance number. FID=1: Indicates the user fingerprint SN. Valid=1: Indicates whether current fingerprint is valid. TMP=.... ... : Indicates the fingerprint template of the BASE64 code.
OPLOG	Administrator operation log	Operation log Administrator ID Time Operation object 1 ** Operation object 2 Operation object 3 Operation object 4

Table 2-4

Description:

1. ID card number format: The square bracket [","] encloses either complete card number data in hexadecimal format or the same number as displayed on the screen when you slide your card.

2. Four "operation objects" in the operation log: Indicate parameters relevant to an operation, as shown in Figure 2-5.

Operation Code	Operation Content	Parameter Description
0	Power on the attendance machine.	
1	Power off the attendance machine.	
2	Fail the verification.	If you adopt the 1:1 verification, "operation object 1" indicates your PIN number.
3	Generate an alarm.	"Operation object 1" indicates specific causes. The possible values contain: 50: Door Close Detected 51: Door Open Detected 55: Machine Been Broken 53: Out Door Button 54: Door Broken Accidentally 58: Try Invalid Verification 65535: Alarm Cancelled
4	Enter the menu.	
5	Modify the configuration.	"Operation object 1" indicates the configuration item SN to be modified. "Operation object 2" indicates the value already modified.
6	Enroll a fingerprint.	"Operation object 1" indicates the user ID. "Operation object 2" indicates the fingerprint SN. "Operation object 3" indicates the fingerprint template size.
7	Enroll a password.	
8	Enroll an HID card.	
9	Delete a user.	"Operation object 1" indicates the user ID.
10	Delete a fingerprint.	"Operation object 1" indicates the user ID.

Operation Code	Operation Content	Parameter Description
11	Delete a password.	“Operation object 1” indicates the user ID.
12	Delete an RF card.	“Operation object 1” indicates the user ID.
13	Purge the data.	
14	Create an MF card.	
15	Enroll an MF card.	
16	Register an MF card.	
17	Delete the MF card registration.	
18	Clean the MF card contents.	
19	Move registration data to the card.	
20	Copy card data to the attendance machine.	
21	Set the time.	
22	Factory setting	
23	Delete the entry/exit records.	
24	Clean the administration privilege.	
25	Modify the access control group settings.	
26	Modify the user access control settings.	
27	Modify the access control time segment.	
28	Modify the unlocking combination settings.	

Operation Code	Operation Content	Parameter Description
29	Perform unlocking.	
30	Enroll a user.	
31	Modify the fingerprint attribute.	
32	Duress alarm.	

Table 2-5

The server returns:

OK

3. Update the Onsite Photo

If the attendance machine is configured with a camera to support onsite photo collection and uploading functions, it can collect onsite photos during user authentication, and upload those photos to the server.

The equipment sends:

```
POST /iclock/cdata?SN=xxxxxx&table=ATTPHOTO&Stamp=99999999
PIN=iid
SN=xxxxxx
size=ssss
CMD=type\0BINARY IMAGE DATA
```

Where:

SN=xxxxxx: Indicates the equipment SN.

table=ATTPHOTO: Indicates the attendance photo table name of current firmware of standard configurations (see Table 2-2).

PIN=iid: Indicates a unique image ID that supports two formats:

PIN=DATETIME-U: DATETIME indicates the user authentication time in YYYYMMDDHHNNSS format. U indicates the user attendance number. This format indicates that user authentication passes.

PIN=DATETIME: Indicates that user authentication fails.

Stamp=285528079: Indicates the timestamp tag of this photo. The server records this timestamp to ATTPHOTOStamp (see Table 2-2) for this equipment to easily return the read configuration information.

size=ssss: Indicates the photo file size.

CMD=type: Indicates the photo transmission type. CMD=uploadphoto indicates that the photo is transmitted through the background. CMD=realupload indicates that the photo is transmitted in realtime.

\0: Indicates the C language string zero terminator.

BINARY IMAGE DATA: Indicates binary contents of onsite photos in .jpg format.

The server returns:

```
OK
```

4. Send a Command From the Server

All commands sent from the server to the equipment will be buffered first rather sent to the peer end immediately. According to the configuration, the equipment will periodically (commonly every 30 seconds) send the following request to the server for checking whether the server sends any commands to itself.

```
GET /iclock/getrequest?SN=xxxxxx
```

Where, xxxxxx indicates the equipment SN.

Upon receipt of this request, the server returns buffered commands to the equipment.

```
C:ID1:CMD1
C:ID2:CMD2
C:ID3:CMD3
```

The server can return multiple commands at a time. The total number of returned commands must not exceed 200 and the total lengths must not exceed 40 KByte. Those commands are divided into multiple lines, each beginning with a "C:". IDx indicates the SN of this command and is used to uniquely identify all commands. CMDx indicates specific command contents and **adopts a line feed character "\n" to mark the end of a command**. The following sections will describe the command set and command formats supported by this system.

After executing the command, the equipment returns the execution results by using the following requests:

```
POST /iclock/devicecmd?SN=xxxxxx
ID=iiii&Return=vvvv&CMD=ssss (This data appears along with the POST command and is not appended to the URL request.) )
```

Where, xxxxxx indicates the equipment SN. POST contains returned results of the command execution . ID=iii indicates the SN corresponding to a command. Return=vvvv indicates the command execution return code. CMD=ssss indicates additional data returned after the command execution. When the command execution return code equals 0, the command execution succeeds; if it equals -1, the command execution fails. For other values, see specific command explanation.

Upon receipt of this request, the server thinks that the corresponding command is already executed and can be cleared from the command buffer.

Note 1: All commands are not immediately transferred from the server to the equipment. To address the problem, the system must send an R-CMD message to the UDP 4374 port of the equipment simultaneously when buffering data on the server. This mechanism greatly accelerates the response speed of server command delivery. It, however, is only applicable to situations where the server can directly connect to the equipment, for example, the equipment possesses an IP address of the public network on the LAN or Internet.

Note 2: When the equipment requests for commands from the server for the first time or the equipment has new registered users or fingerprints and new attendance records, the URL path format contains basic information items including INFO=Hardware version number, number of registered users, fingerprints, and attendance records, and attendance machine IP address.

```
GET     http://host/iclock/getrequest?SN=xxxx&INFO=Ver
6.39 Apr 28 2008,2,0,0,192.168.1.201
```

Commands from Server to Equipment

1. Execute system commands

Format:

SHELL CMD_String

Function:

Execute system commands.

Return value:

1) When a system command is executed successfully, the returned data is in the following format:

```
ID=iiii
SN=xxxx
Return=vvvv
CMD=Shell
FILENAME=shellout.txt
Content=ssss
```

Where, vvvv is the return value of the system command and ssss is the output content (probably multi-line text) after command execution.

2) When a system command is executed unsuccessfully or in incorrect format, the returned data format is ID=iiii&Return=-1&CMD=Shell.

2. Check data update

Format:

CHECK

Function:

The equipment needs to read its configuration information from the server and then check whether any data is updated on the equipment itself. If so, the equipment must send new data to the server instantly.

Return data:

The POST content is ID=iiii&SN=xxxx&Return=0&CMD=CHECK.

3. Clear data

Format 1:

CLEAR LOG

Function:

Clear attendance logs.

Format 2:

CLEAR DATA

Function:

Clear all data.

Format 3:

CLEAR PHOTO

Function:

Clear the onsite collected photos.

Return data:

The POST content is ID=iiii&Return=0.

4. Send equipment information to server

Format:

INFO

Return data:

If this command is executed successfully, the equipment POST content is:

```
ID=iiii&Return=0&CMD=INFO
OPTIONS
```

OPTIONS indicates equipment information and valid configuration items and contains multi-line text. Each line is in the format “Item=Value”. These configuration items include:

Item	Meaning
TransactionCount	The number of current attendance logs
FPCount	The number of registered fingerprints
UserCount	The number of registered users
FWVersion	Firmware version number

Item	Meaning
……	……

For details of other items, see Set equipment options command.

5. Set equipment options

Format:

SET OPTION ITEM=VALUE

Where, ITEM is the option content and VALUE is the option value. For example:

SET OPTION IPAddress=192.168.1.225

Set the IP address of the equipment to 192.168.1.225.

Currently the supported items are listed in the following table:

Item	Meaning
IPAddress	IP address of the equipment
NetMask	Subnet mask of the equipment
GATEIPAddress	Gateway address of the equipment
VOLUME	Volume
MAC	Ethernet MAC address of the equipment. C language format: "%02X:%02X:%02X:%02X:%02X:%02X".
CardKey	Mifare card encryption key
DeviceID	Equipment ID number
LockOn	Unlocking duration
AlarmAttLog	Attendance log alarm
AlarmReRec	Minimum repetitive attendance recording interval
RS232BaudRate	RS232/RS485 baud rate
AutoPowerOff	Automatic power-off time. Format: hour ×

Item	Meaning
	256 + minute The following time setting items all adopt this format.
AutoPowerOn	Automatic power-on time
AutoPowerSuspend	Automatic standby time
AutoAlarm1~AutoAlarm50	50 automatic timing alarms
IdlePower	Idle setting
IdleMinute	Idle duration (minute)
RS232On	Whether to enable the RS232 connection
RS485On	Whether to enable the RS485 connection
UnlockPerson	The number of users unlocking the door
OnlyPINCard	Only read the Mifare card ID number.
HiSpeedNet	Network rate
Must1To1	Whether to allow only 1:1 fingerprint matching
ODD	Unlock time. If the door still remains open over the due time, an alarm will be generated.
DSM	
AADelay	
DUHK	Whether to enable the emergency call function in the case of duress alarm
DU11	Duress alarm generated at 1:1 fingerprint matching

Item	Meaning
DU1N	Duress alarm generated at 1:N fingerprint matching
DUPWD	Duress alarm generated at password verification
DUAD	Duress alarm latency (second)
LockPWRButton	Lock the power-off button
SUN	Whether to send a broadcast message at equipment power-on to help other computers on the same network find the current equipment
I1NFrom	Set a start user number in 1:N fingerprint matching mode
I1NTo	Set an end user number in 1:N fingerprint matching mode
I1H	Whether to enable the 1:H function
I1G	Whether to enable the 1:G function
KeyPadBeep	Whether to beep with every keystroke
WorkCode	Whether to enable the WorkCode function
AAVOLUME	Alarm volume
DHCP	Whether to enable the DHCP function
EnableProxyServer	Whether to enable the HTTP proxy server
ProxyServerIP	IP address of the HTTP proxy server
ProxyServerPort	Port of the HTTP proxy server
PrinterOn	Whether to enable the printer

Item	Meaning
DefaultGroup	Default group number
GroupFpLimit	Limit of the number of fingerprints in each group
WIFI	Whether to enable WiFi
wifidhcp	Whether to enable the DHCP function of WiFi
AmPmFormatFunOn	Whether to display AM/PM on the main interface
AntiPassbackOn	Whether to enable the anti-passback function
MasterSlaveOn	Whether to enable the master/slave function
ImeFunOn	Whether to enable the T9 input method
WebServerIP	IP address of the PUSH SDK Web server
WebServerPort	Port number of the PUSH SDK Web server
ApiPort	Port number of DataAPI SDK
DelRecord	The number of history attendance records automatically deleted when the total number of records exceeds the maximum limit.

Note: Some items are supported only by specific equipment. For example, AntiPassbackOn is supported only by some devices with the advanced access control function; WIFI can be enabled only on the devices with built-in WiFi module.

Return data:

The POST content is ID=iiii&SN=xxxx&Return=0&CMD=SET OPTION.

6. Reboot

Format:

REBOOT

Function:

Reboot the equipment.

Note:

If the server returns several commands to the equipment, the **REBOOT** command must be the last one; otherwise, the subsequent commands will be neglected.

7. Data command

Format:

DATA <SUBCMD>

<SUBCMD> includes the following subcommands:

USER tablename value: This subcommand is used to update or modify data in tablename table.

DEL_USER tablename key: This subcommand is used to delete data from tablename table according to key

QUERY tablename key: This subcommand is used to query tablename table data according to key

For table names, see Table 2-2.

1) Add or modify a user profile:

DATA USER PIN=

%d\tName=%s\tPri=%d\tPasswd=%s\tCard=[%02x%02x%02x%02x%02x]\tGrp=%d\tTZ=%d

For meanings of all fields, see the following:

DATA: Data adding or modification

USER: Data table name

PIN: A user ID

Name: A user name.

Pri: Privileges (1: Administrator; 0: Ordinary user). Passwd: A user password

Card: A user ID card number

Grp: A user group (used for access control)

TZ: Time segment (used for access control)

In the command, only PIN is mandatory, and the rest are optional.

Return value description:

0 indicates successful command execution

-1 indicates a parameter error

-3 indicates an access error

2) Add or modify a user fingerprint.

DATA FP PIN=%d\tFID=%d\tSize=%d\tValid=%d\tTMP=%s

(Original command: FP PIN=%d\tFID=%d\tSize=%d\tValid=%d\tTMP=%s)

For meanings of all fields, see the following:

DATA: Data adding or modification.

FP: Data table name.

PIN: A user ID.

FID: Fingerprint template number.

Size: Fingerprint template size (this one does not exist in previous protocols).

Valid: 1 indicates valid, 0 indicates invalid.

TMP: A fingerprint template.

Return value description:

0 indicates successful command execution

-1 indicates a parameter error

-3 indicates an access error

-9 indicates that fingerprint template does not match the given size (this feature is not supported in previous versions, and the fingerprint template size check is added into the current version).

-10 indicates that the user with the specified PIN does not exist in equipment, and relevant operations can only be performed after this user is added by running the **DATA USER** command.

-11 indicates an invalid fingerprint template format.

-12 indicates an invalid fingerprint template.

Delete specified users and their fingerprints

DATA DEL_USER PIN=%d

Field explanation:

DEL: Delete data.

USER: Name of the data table to be operated.

Return value description:

0 indicates successful command execution

-1 indicates a parameter error

-3 indicates an access error

4) Delete a user fingerprint

DATA DEL_FP PIN=%d\tFID=%d

Return value description:

0 indicates successful command execution

-1 indicates a parameter error

-3 indicates an access error

5) Upload profile of specified user

QUERY USERINFO PIN=%d

All users' profile will be uploaded if no PIN is specified.

Field explanation:

QUERY: Query data.

Return value description:

0 indicates successful command execution

-1 indicates a parameter error

-3 indicates an access error

6) Upload fingerprint template of a specified user

QUERY FINGERTMP PIN=%d\tFingerID=%d

Return value description:

0 indicates successful command execution

-1 indicates a parameter error

-3 indicates an access error

7) Download a user photo

UPDATE USERPIC PIN=%d\tPIN2=%d PICFILE=%s

Return value description:

0 indicates successful command execution

-1 indicates a parameter error

-3 indicates an access error

8) Delete a user photo

DELETE USERPIC PIN=%d

Return value description:

0 indicates successful command execution

-1 indicates a parameter error

-3 indicates an access error

9) Query the attendance records within a specified time segment

QUERY ATTLOG StartTime=%s\tEndTime=%s

Return value description:

0 indicates successful command execution

-1 indicates a parameter error

-3 indicates an access error

10) Query the attendance photos within a specified time segment

QUERY ATTPHOTO StartTime=%s\tEndTime=%s

Return value description:

0 indicates successful command execution

-1 indicates a parameter error

-3 indicates an access error

11) Add or modify time zone

UPDATE TIMEZONE TZID=%d\tITIME=%s\tRESERVE=%s

Return value description:

0 indicates successful command execution

-1 indicates a parameter error

-3 indicates an access error

12) Delete a time zone

DELETL TIMEZONE TZID=%d

Return value description:

0 indicates successful command execution

-1 indicates a parameter error

-3 indicates an access error

13) Add or modify unlocking combination

UPDATE GLOCK GLID=%d\tGRO UPIDS=%s\tMEMBERCOUNT=%d\tRESERVE=%s

Return value description:

0 0 indicates successful command execution

-1 -1 indicates a parameter error

-3 -3 indicates an access error

14) Delete unlocking combination

DELETE GLOCK GLID=%d

Return value description:

0 indicates successful command execution

-1 indicates a parameter error

-3 indicates an access error

15) Send an SMS message

Format:

UPDATE SMS MSG=%s\tTAG=%d\tUID=%d\tMIN=%d\tStartTime=%s

MSG indicates the to-be-displayed SMS message.

TAG: 253 indicates an SMS notification, and 254 indicates a user SMS message.

UID indicates the specified SMS ID;

MIN indicates the validity period (minutes) of an SMS message

StartTime indicates the validity period of an SMS message, and the format is YYYY-MM-DD HH:NN:SS (YYYY: Year; MM: Month; DD: Day; HH: Hour; NN: Minute; SS: Second).

Function:

Update equipment SMS messages. SMS messages are displayed according to the table

Back:

Return value is the size of downloaded file (bytes).

```
UPDATE USER_SMS PIN=%d\tUID=%d
```

Function:

Update personal SMS message user list

Return value description:

0 indicates successful command execution

-1 indicates a parameter error

-3 indicates an access error

8. Reload system options

Format:

```
RELOAD OPTIONS
```

Function:

The modified system options do not take effect unless the system configurations and options are reloaded.

Return value:

The return value of POST is ID=iiii&SN=xxxx&Return=0

9. Enroll a user fingerprint

Format:

```
ENROLL_FP PIN=%d\tFID=%d\tRETRY=%d\tOVERWRITE=%d
```

PIN indicates a user ID.

FID indicates a user fingerprint ID.

RETRY indicates retry times.

OVERWRITE: indicates whether to overwrite previous fingerprints (1: Overwrite; 2: Not Overwrite)

Function:

Initiate fingerprint enrollment.

Note:

{This function may not be available for some models. Return value description:

0 indicates a successful registration. 2 indicates the user fingerprint already exists.

6 indicates registration cancellation

5 indicates the registered fingerprint already exists in fingerprint database (fingerprint repetition)

{4 indicates registration failure. Normally, this is either due to poor fingerprint quality or because you have input incorrect fingerprints in three consecutive times.

10. Check and upload new data

Format:

LOG

Function:

Check whether there is new data. If there is, upload the new data to server immediately.

Return value description:

The return value of POST is ID=iii&Return=0&CMD=LOG

Output a unlocking signal

Format:

AC_UNLOCK

Function:

The access control equipment outputs a unlocking signal.

Return value description:

The return value of POST is ID=iii&Return=0&CMD=LOG

Cancel alarm signal output

Format:

AC_UNALARM

Function:

The access control equipment cancels alarm signal output.

Return value description:

The return value of POST is ID=iii&Return=0&CMD=LOG

Obtain files in the equipment

Format:

GetFile FilePath

Function:

The equipment sends system file FilePath to server. The file path is specified by FilePath.

Return value description:

POST return value:

```
ID=1234

SN=99999

FILENAME=FilePath

CMD=GetFile

Return=999

Content=ssss
```

Where,

ID=1234 is command ID

SN=999999 is equipment serial number

FILENAME=FilePath is file name

Return=999 indicates the size of file (bytes)

Content=ssss is file content ssss is either multi-line text or binary content.

14. Send files to equipment

Format:

PutFile URL FilePath

Function:

Download the file from the server, and save the downloaded file to a directory specified by FilePath (for a **.tgz** file, the equipment will automatically untar it to a directory specified by FilePath. If the directory is not specified, it will untar the **tgz** file under the **/mnt/mtdblock** directory. For files of other formats, the file path and file name must be specified).The file must be downloaded over HTTP from the server, and the URL for the file must be given.

If the URL starts with **http:** //, the equipment will deem it as a complete URL address. Otherwise, the /iclock/ of the server will be added to a specified URL by the equipment. Fro example:

PutFile file/fw/X938/main.tgz main.tgz

or

PutFile file/fw/X938/main.tgz

Download main.tgz from http://server/iclock/file/fw/X938/main.tgz, and untar it to the **/mnt/mtdblock** directory.

PutFile file/fw/X938/main.tgz /mnt/

Download main.tgz from http://server/iclock/file/fw/X938/main.tgz, and untar it to the **/mnt/** directory.

PutFile file/fw/X938/ssruser.dat /mnt/mtdblock/ssruser.dat

Download ssruser.dat from http://server/iclock/file/fw/X938/ssruser.dat, and save it to the **/mnt/mtdblock/ssruser.dat** directory.

Return value description:

Return value is the size of downloaded file (bytes).