Specification file of Remote Identification Server
Contents

I. Preface..................................................................................................................3

II. Installing remote identification server and URU fingerprint reader driver.........................................................6

III. Fingerprint registration ..............................................................................7

  3.1 User management......................................................................................7
  3.2 Device management................................................................................8
  3.3 Database settings......................................................................................9

IV. Connection of A5 and fingerprint remote identification server ..............................................................................10

V. System settings............................................................................................11

  5.1 Database..................................................................................................11
  5.2 Network ..................................................................................................12
  5.3 Remote identification .............................................................................13
  5.4 Record display .........................................................................................14

VI. Remote identify server personnel configuration ..................15

  6.1 Zone management .................................................................................15
  6.2 Remote identify server management .................................................16
  6.3 Personnel group management ............................................................17
  6.4 Zone configuration management ........................................................18
  6.5 Operation user management ..............................................................19

VII. Quick use guide ..........................................................................................20
I. Preface

For the following reasons, the traditional attendance methods cannot meet the demand of large-scale enterprises: Abroad area, an enterprise scale can be distributed in N areas; Large number of employees, an middle scale enterprise can include over thousands of employees; Strong fluidity, employees of an enterprise can work in many areas, e.g. employees in A area can work in B area for some time or transfer into B area after working for some time in A area. In the above situation, it will take many people and much time to count and process the attendance result when use conventional attendance method. Facing so mush & complex work, we have purpose to build a set of complete attendance network for enterprises through which the attendance data of all employees in an enterprise can be stored in a large database so that employees of any terminal can be kept attendance records, i.e. Front End Matching & Background identification, therefore the original attendance records of all employees will be stored in the database. What has illustrated in above is also the design idea of remote identification server, where as the main function of remote identification server can be summarized as the following:

1. Remote user register, user information enrolls.
   After building remote identification server successfully, the administrator can enroll fingerprint or ID card of enterprise employees in any terminal and enter user information in identification server.
2. Domain Management
   Maybe the scope of an enterprise can be distributed in several domains; therefore we can divide them into N domains and build remote identification server in the domains. Personnel are movement, but not are the domain; this is the relationship between domain and personnel. In this situation, we can set a cycle of personnel movement, 28 days in default, which means that when the attendance record of personnel in flowing group of an domain exceeds 28 days, he/she will be added into the personnel of fixed group in this domain automatically.
3. Remote identification and Server Management
   In one domain there are several remote identification servers, so you can manage them, such as change the name or IP address of remote identification server, create new remote identification server or delete existing remote identification server.
4. Personnel Grouping Management
   The newly registered users in remote identification server will be defaulted as users of flowing group. The administrator can group the users in the domain and furthermore add users of flowing group into fixed group. In addition, the administrator can also add or change the grouping depending on the enterprise requirement.
5. Domain configuration management
   Remote identification server and personnel group corresponding to the domain can be configured.

Following is the figure of network structure of remote identification server:
Following is the workflow of remote identification server:

![Diagram of remote identification server workflow]

Figure of personnel flow:
II. Installing remote identification server and URU fingerprint reader

Put the CD of remote identification server into CD-ROM and the Dialog box will appear. Please select desired langue and click OK as following:

Then you will enter into the Welcome Interface of installing fingerprint remote identification server, please click next to enter Protocol of installing fingerprint remote identification. Here select Agreement and click Next to select path as following:

To change the path, you can change the path here directly. Then click next until Install appears, click it and click Completed when the install completes.

Then URU fingerprint reader driver must be installed because it is adopted by all the A5 fingerprint readers.
III. Fingerprint registration

Because remote service matches in the front end and identify in the background, we recommend users to use URU to register all the user registrations into server base directly and remote registration is an auxiliary registration method. Open the desk shortcut “Fingerprint registration”, and a dialogue box as below for administrator confirm pops up:

![Log On Dialogue Box]

Default user code and password are “admin”. Enter the following selection menu after confirming the administrator.

![User Information Maintenance Dialogue Box]

3.1 User management

Enter “User management”. In the User management, on the left is the user list and on the right is user maintenance Area Click “+” or “-” to add or delete a user. Also other information such as name, gender and position can be controlled here.

“Department management” can add a department. Use drop-down arrow to move related personnel to corresponding department after adding a new department.
For fingerprint management, we recommend users to use URU fingerprint sensor. After installing URU properly, click “Register”, and a fingerprint registration interface pops up. Registration is successful or failing after three finger presses. There is another auxiliary registration method that is to press fingerprint on the terminal after connecting the terminal.

To Transit user information and related fingerprint. It is available to upload the user information and related fingerprint to the terminal and download them to remote identification server database. This is an emergency function of remote identification server. Because we cannot make sure there is no accident for remote identification sever network, we use this method to upload the fingerprint to the terminal. When accident occurs in the remote identification severs the terminal will automatic switch to offline matching mode.

3.2 Device management

Device management is to manage and maintain the terminal. After opening Device management, you can set all the parameters for standalone device as below:
3.3 Database settings

For remote identification server, it is recommended to use SQL database that is safe and convenience. We supply many kinds of database ports, such as SQL, Oracle and DB.
IV Connection of A5 and fingerprint remote identification server

1. Firstly we consider A5 as a terminal of the entire enterprise local area network (LAN) and distribute an IP address to it, than modify this IP address in the communication settings directly.

2. Use an independent PC in the enterprise LAN for remote identifies server. Therefore select “Yes” for background remote identification in the advanced option of A5 system option, and then input the PC’s IP address of remote identification server.

When running remote identification server for the first time, the prompt of configuration personnel information will pop up as below:

![Image](image1.png)

Click “OK” to enter main interface of fingerprint remote identification server. It is required that there is no default in the remote identification service network. In this case after starting remote identification service; it will start to connect with A5 as below:

![Image](image2.png)

In this way, fingerprint can be registered in A5 long distance.
V. System settings

After starting remote identification server, click “System settings” in the main interface, and then an administrator dialogue box pops up as below, among default administrator user and password are “admin”.

![Log On](image)

5.1 Database

Database connects the parameter settings of property, personnel information and fingerprint data as below:

![System Option](image)

Set database connection. Database connection supplies several usual database ports, such as DB, SQL and Oracle. The installation disk has a script file.

Local buffer personnel information and fingerprint data. Here can set cycle time to refresh flowing personnel data automatically. The default time is 1 hour, which is to add the personnel floating of 1:1-matching fingerprint to the local machine per hour.

Whether start refresh personnel information and fingerprint data automatically and whether designate firmware cycle time to refresh personnel information and fingerprint data automatically are determined by users.
5.2 Network

Remote identification server ports are unified to be “4368”.
Rectify IP. If the IP address of remote identification server needs to rectify, you can rectify the IP here.
UDP ports are unified to be “4371”.
The quantity of corresponding remote identification terminals is “3” and the maximum subsequent remote identification quantity is “5”.
When operating system starts, it will run automatically. If select this option, the fingerprint remote identification server will start and run automatically after the operating system starts.
The refresh cycle time of remote identification server idle is 3 hours by default and also can be customized by users.
Time range to justify remote identification of remote identification server idle is 30 minutes by default and also can be customized by users.
5.3 Remote identify

Registration times: Indicates the required registration times in case of remote fingerprint registration. The default times are 3 and can be set to 4 times at most.

Remote registration overtime (second), In case of remote fingerprint registration, the period between previous finger press and next finger press is remote registration overtime. The default overtime is 1 minute, which means that it will automatically pop up fingerprint registration menu if there is no next finger press within 1 minute after the previous finger press.

1: N- and 1:1-matching threshold value is adjusted by an administrator according to matching pass rate.

Display fingerprint figure: Indicates whether display fingerprint figure or not in the main interface in the case of remote identification server matching fingerprint after running.

Save remote identification records: Remote identifies record is the remote identification information record saved in the main interface of the remote identification server.
### 5.4 Record display

The administrator can rectify all the communication parameters here in the main interface of the remote identification server according to practical requirements.

![System Options](image)

<table>
<thead>
<tr>
<th>Database</th>
<th>Network</th>
<th>Identification</th>
<th>Record the displayed options</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Connect Request</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Command Request</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Staff Information</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Other Data</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Score</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>accept data size</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>time that Receive the image</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>identification time-consuming</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Reply Data</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>UDP Data</td>
</tr>
</tbody>
</table>
VI. Remote identification server personnel configuration

When opening “Remote identification server personnel configuration”, also need to validate administrator identity. The default administrator and password are “admin”.

6.1 Zone management

In domain management, you can rectify zone name and set personnel flowing parameters as below:
The flowing personnel in the zone usually are those who work here from other domain in the enterprise and have attendance record. The system can set flowing cycle time in the zone and the default value is 28 days, which means the system will rectify the flowing personnel to fixed-group personnel automatically if those personnel remains here exceeding 28 days. In this case, the flowing personnel have been in fixed group in the domain.

6.2 Remote identification server management

A remote identification server can connect several terminals. A domain also can have several remote identification servers. For remote identification server, we can maintain them, such as add, rectify or delete.
6.3 Personnel group management

After remote fingerprint registration, enter to personnel group management to list all the users and fingerprints of remote registration to the remote identification server to the personnel information list. Here, you can add, rectify or delete a group. In addition, user fingerprint with a low pass rate can be set to be a difficult one, and difficult fingerprint inquiry also can be set. Group all the personnel in the domain to the firmware group in the zone. First select “Default domain flowing group”, and then click “Personnel grouping”, and the management interface of personnel grouping pops up as below:
Move the left flowing personnel to the right user list, click “OK”, and then click “Memory settings”.

6.4 Domain configuration management

The system is managed by the way of domain. Specific remote identification servers and personnel groups corresponding to the zone can be configured here.
6.5 Operation user management

The system super administrator code and password are “admin”. For security, you can rectify user and password. In addition, you can add operation administrator with different rights according to the rights in the “right” list.
VII. Quick use guide

Remote identification server is easy-to-operate and the entire networking environmental connection is very simple. Proceeds as below:

I. Hardware networking connection

Remote identification means matching in the front end and remote identify in the back ground and all the terminals are connected to the same background server database. Remote identification server enables to connect the front end with the background through TCP/IP. So the effective IP address should be distributed to all the terminals (A5) connected to the remote identification to connect the b remote identification terminal with the network in the zone, ensuring network working normally. Proceeds as bellow:

1. Configure and install all the terminals

In this procedure, it is mainly that the user configures reasonably and installs all the terminals according to practical situation. Most importance is comprehensive wiring to enable the networks of all the terminals default-free.

2. Configure background remote identification parameters for all the terminals

In the “Communication settings”, set the effective IP address in the zone LAN. Note the address cannot conflict with any terminal IP address and the terminal machine number cannot repeat.

In the “Advanced option” of “System option”, change the “Remote identification service” option to “Yes”, and set “Validate server address”, exit and save the settings, and restart the terminal.

II. Install software and URU fingerprint reader drive, and configure the system settings of remote identification server.

III. Fingerprint registration

Open “Use management”, enter “User management”, click the right “+” to register users. For remote identification service, we recommend to use URU fingerprint registration reader to register fingerprint. Use fingerprint reader to register all the users’ fingerprint to the remote identification server database, and then restart remote identification server to do front-end and background remote identification. Generally, the user numbers of remote identification server is relatively large. In this case, the requirement of fingerprint quality is relatively high to prevent from error. So URU fingerprint reader is the optical choice and A5 remote registration is only an auxiliary method.

IV. Personnel configuration of remote identification server

It mainly includes personal grouping, remote identification server management, zone management, zone configuration management and operation user management. The most importance is personnel grouping, which means to add the users registered in flowing group to the fixed group.

After registering all the personnel, open “Remote identification server personnel configuration”, enter “Personnel group management” to group the personnel. In default settings, registered users for the first time are considered to be in movement group. Administrators can add the effective users to the movement group according to practical situation.