Synway®

Synway SMG Series SR Gateway

SR500 Gateway

User Manual

Version 1.8.0

Synway Information Engineering Co., Ltd

www.synway.net

Content

Copyright Declaration

Revision History

Version	Date	Comments
Version 1.6.4	2016-10	Initial publication
Version 1.6.5	2017-06	New revision
Version 1.7.0	2018-06	New revision
Version 1.8.0	2019-12	New revision

Note: Please visit our website http://www.synway.net to obtain the latest version of this document.

Chapter 1 Product Introduction

Thank you for choosing the Synway SR500 gateway products!

Cooperating with the Synway SMG series digital gateways, the SR500 series call classification equipment, as a screen server, performs voice recognition on the called party of the digital gateway, analyzes the called status such as empty number, turnoff, out of operation, etc., and returns the result to the digital gateway.

1.1 Typical Application

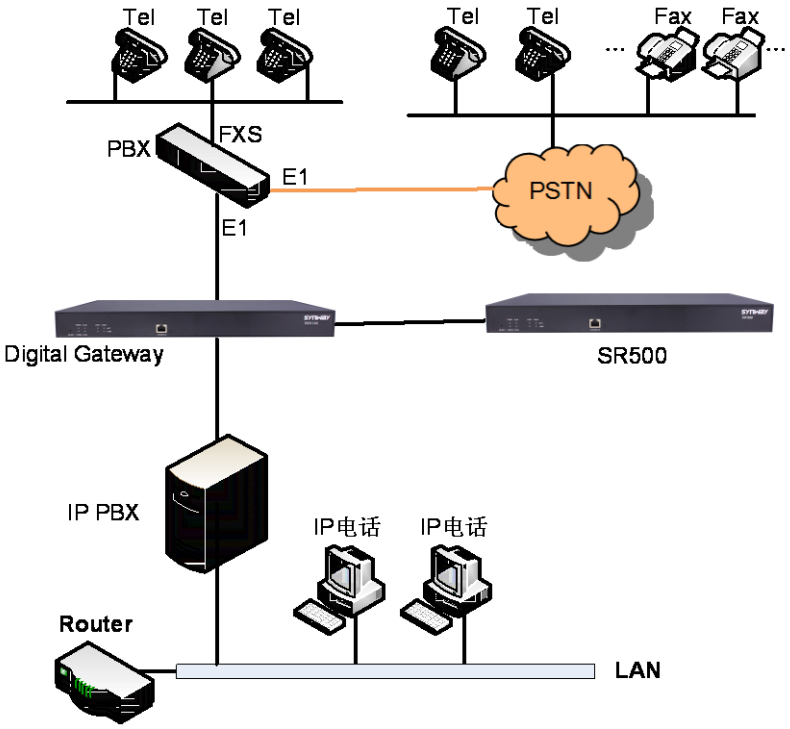

Figure 1-1 Typical Application

1.2 Feature List

Basic Features	Description
Number Screening	Perform voice recognition on the called party of the digital gateway, obtaining the called status such as empty number, turnoff, out of operation, etc.
Network	**Description**
Network Protocol	Supported protocol: TCP/UDP, HTTP, ARP/RARP, DNS, NTP, TFTP, TELNET, STUN
Static IP	IP address modification support
DNS	Domain Name Service support
Security	**Description**

Admin Authentication	Support admin authentication to guarantee the resource and data security
Maintain & Upgrade	**Description**
WEB Configuration	Support of configurations through the WEB user interface
Language	Chinese, English
Software Upgrade	Support of user interface, gateway service, kernel and firmware upgrades based on WEB
Tracking Test	Support of Ping and Tracert tests based on WEB
SysLog Type	Three options available: ERROR, WARNING, INFO

1.3 Hardware Description

The SR500 gateway features 1U rackmount design and integrates embedded LINUX system within the POWERPC+DSP hardware architecture. It has 2 Kilomega-Ethernet ports on the chassis. See the figures below for its appearance:

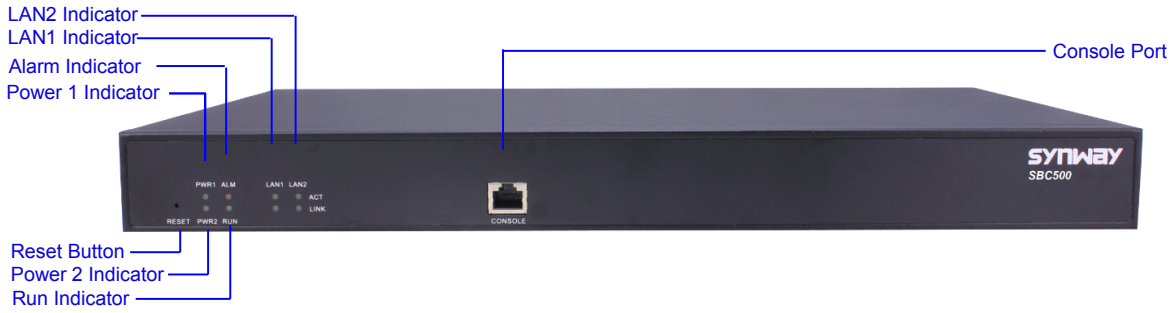

Figure 1-2 Front View

Figure 1-3 Rear View

Figure 1-4 Left View

The table below gives a detailed introduction to the interfaces, buttons and LEDs illustrated above:

Interface	Description
LAN	Amount: 2

	Type: RJ-45
	Bandwidth: 10/100/1000Mbps
	Self-Adaptive Bandwidth Supported
	Auto MDI/MDIX Supported
Console Port	Amount: 1
	Type: RS-232
	Baud Rate: 115200 bps
	Connector: RJ45 (See Figure 1-5 for signal definition)
	Data Bits: 8 bits
	Stop Bit: 1 bit
	Parity Unsupported
	Flow Control Unsupported
Button	**Description**
Power Key	Power on/off the SR500 gateway. You can turn on the two power keys at the same time to have the power supply working in the hot-backup mode.
Reset Button	Restore the gateway to factory settings.
LED	**Description**
Power Indicator	Indicates the power state. It lights up when the gateway starts up with the power cord well connected.
Run Indicator	Indicates the running status. For more details, refer to Alarm Info.
Alarm Indicator	Alarms the device malfunction. For more details, refer to Alarm Info.
Link Indicator	The green LED on the left of LAN, indicating the network connection status.
ACT Indicator	The orange LED on the right of LAN, whose flashing tells data are being transmitted.

Note: The console port is used for debugging. While connection, the transmitting and receiving lines of the gateway and the remote device should be cross-linked. That is, connect the transmitting line of the gateway to the receiving line of the remote device, and vice verse. The figure below illustrates the signal definition of the console port on the gateway.

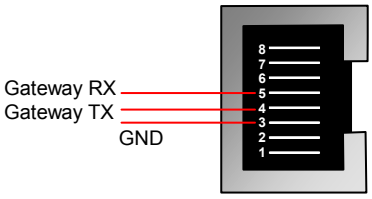

Figure 1-5 Console Port Signal Definition

For other hardware parameters, refer to Appendix A Technical Specifications.

1.4 Alarm Info

The SR500 gateway is equipped with two indicators denoting the system's running status: Run Indicator (green) and Alarm Indicator (red). The table below explains the states and meanings of the two indicators.

LED	State	Description
Run Indicator	Go out	System is not yet started.
	Light up	System is starting.

	Flash	Device is running normally.
Alarm Indicator	Go out	Device is working normally.
	Light up	Upon startup: Device is running normally. In runtime: Device goes abnormal.
	Flash	System is abnormal.

Note:

- The startup process consists of two stages: System Booting and Gateway Service Startup. The system booting costs about 1 minute and once it succeeds, both the run indicator and the alarm indicator light up. Then after the gateway service is successfully started and the device begins to work normally, the run indicator flashes and the alarm indicator goes out.
- During runtime, if the alarm indicator lights up or flashes, it indicates that the device goes abnormal. If you cannot figure out and solve the problem by yourself, please contact our technicians for help. Go to Appendix C Technical/sales Support to find the contact way.

Chapter 2 Quick Guide

This chapter is intended to help you grasp the basic operations of the SR500 gateway in the shortest time.

Step 1: Confirm that your packing box contains all the following things.

- SR500 Series Gateway *1
- Angle Bracket *2, Rubber Foot Pad *4, Screw for Angle Bracket *8
- 220V Power Cord *2
- Warranty Card *1
- Installation Manual *1

Step 2: Properly fix the SR500 gateway.

If you do not need to place the gateway on the rack, simply fix the 4 rubber foot pads. Otherwise, you should first fix the angle brackets onto the chassis and then place the chassis on the rack.

Step 3: Connect the power cord.

Make sure the device is well grounded before you connect the power cord. Check if the power socket has the ground wire. If it doesn't, use the grounding stud on the rear panel of the device (See Figure 1-3) for earthing.

Note: Each SR500 gateway has two power interfaces to meet the requirement for power supply hot backup. As long as you properly connect and turn on these two power keys, either power supply can guarantee the normal operation of the gateway even if the other fails.

Step 4: Connect the network cable.

Step 5: Log in the gateway.

Enter the original IP address (LAN 1: 192.168.1.101 or LAN 2: 192.168.0.101) of the SR500 gateway in the browser to go to the WEB interface. The original username and password of the gateway are both 'admin'. For detailed instructions about login, refer to System Login. We suggest you change the initial username and password via 'System Tools → Change Password' on the WEB interface as soon as possible after your first login. For detailed instructions about changing the password, refer to Change Password. After changing the password, you are required to log in again.

Step 6: Modify IP address of the gateway.

You can modify the IP address of the gateway via 'System Tools → Network' on the WEB interface to put it within your company's LAN. Refer to Network for detailed instructions about IP modification. After changing the IP address, you shall log in the gateway again using your new IP address.

Special Instructions:

- The chassis of the SR500 gateway must be grounded for safety reasons, according to standard industry requirements. A simple way is earthing with the third pin on the plug or the grounding studs on the machine. No or improper grounding may cause instability in operation as well as decrease in lightning resistance.
- As the device will gradually heat up while being used, please maintain good ventilation to prevent sudden failure, ensuring that the ventilation holes (see Figure 1-4) are never jammed.
- During runtime, if the alarm indicator lights up or flashes, it indicates that the device goes abnormal. If you cannot figure out and solve the problem by yourself, please contact our technicians for help. Otherwise it may lead to a drop in performance or unexpected errors.

Chapter 3 WEB Configuration

3.1 System Login

Type the IP address into the browser and enter the login interface. See Figure 3-1.

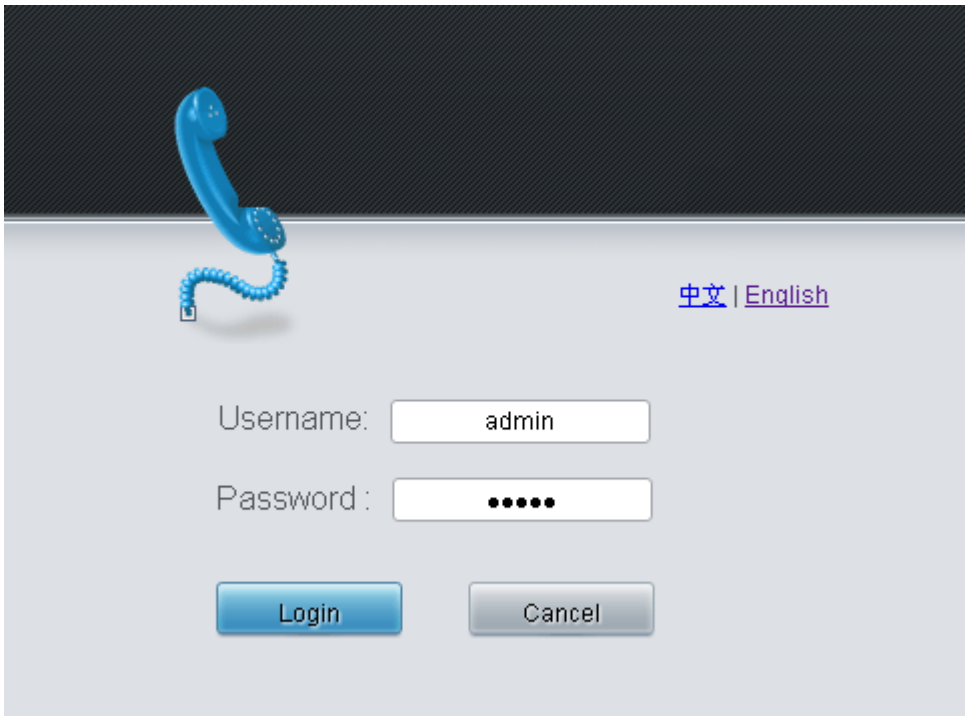

Figure 3-1 Login Interface

The gateway only serves one user, whose original username and password are both 'admin'. You can change the username and the password via 'System Tools → Change Password' on the WEB interface. For detailed instructions, refer to Change Password.

After login, you can see the main interface.

3.2 Operation Info

Operation Info includes two parts: ***System Info*** and ***Warning Info***, showing the current running status of the gateway.

3.2.1 System Info

On the System Info interface, you can click ***Refresh*** to obtain the latest system information. See below for details.

Item	Description
MAC Address	MAC address of LAN 1 or LAN 2.
IP Address	The three parameters from left to right are IP address, subnet mask and default gateway of LAN 1 or LAN 2.
DNS Server	DNS server address of LAN 1 or LAN 2.
Receive/Transmit Packets	The amount of receive/transmit packets after the gateway's startup, including three categories: All, Error and Drop.
Current Speed	The current speed of data receiving and transmitting.

Work Mode	The work mode of the network, including six options: 10 Mbps Half Duplex, 10 Mbps Full Duplex, 100 Mbps Half Duplex, 100 Mbps Full Duplex, 1000 Mbps Full Duplex and Disconnected.
Network Type	The type of the network, including three options: Static, DHCP and PPPoE.
Runtime	Time of the gateway keeping running normally after startup. This parameter updates every 2s.
CPU Temperature	Display the real time temperature of the CPU.
CPU Usage Rate	Display the real time usage rate of the CPU.
Current RTP Message Data	Display the receiving and sending information of the current RTP data.
Authorization Status	Display the features of the SR500 device, which requires authorization.
Authorization Numbers	Display the number of authorized devices.
Remaining Time	Display the remaining time after successful authorization.
Serial Number	Unique serial number of an SR500 gateway.
WEB	Current version of the WEB interface.
Gateway	Current version of the gateway service.
Uboot	Current version of Uboot.
Kernel	Current version of the system kernel on the gateway.
Firmware	Current version of the firmware on the gateway.

3.2.2 Warning Info

The Warning Information interface displays all the warning information on the gateway.

3.3 System Tools

System Tools is mainly for gateway maintenance. It provides such features as IP modification, time synchronization, data backup, log inquiry and connectivity check.

3.3.1 Network

The network settings interface is used to configure parameters about network. A gateway has two LANs, each of which can be configured with independent IP address, subnet mask and default gateway. It supports the DNS server. The Bond feature when enabled will make the information of LAN1 and LAN2 duplicated and backed up so as to realize the hot-backup function between LAN1 and LAN2. By default, this feature is *disabled*.

Note: 1. The two configuration items IP Address and Default Gateway cannot be the same for LAN1 and LAN2.

2. By default, *Speed and Duplex Mode* is hidden, set to Automatic Detection, you can click 'F' to let it display. We suggest you do not modify it because the non-automatic detection may cause abnormity in network interface.

After configuration, click ***Save*** to save the above settings into the gateway or click ***Reset*** to restore the configurations. After changing the IP address, you shall log in the gateway again using your new IP address.

3.3.2 Authorization

On the Authorization Management interface, you can import a trial or formal authorization just by uploading the authorization file which is provided by Synway and cannot be modified. SR500 supports up to 512 channels of authorization.

3.3.3 Management

The table below explains the items shown on the Management Parameters Setting interface.

Item	Description
WEB Port	The port which is used to access the gateway via WEB. The default value is 80.
Access Setting	Sets the IP addresses which can access the gateway via WEB. By default, all IPs are allowed. You can set an IP whitelist to allow all the IPs within it to access the gateway freely. Also you can set an IP blacklist to forbid all the IPs within it to access the gateway.
Time to Log Out	The gateway will log out automatically if it is not operated during a time longer than the value of this item, calculated by s, with the default value of 1800.
SSH	Sets whether to enable the gateway to be accessed via SSH, with the default value of *No*.
SSH Port	The port which is used to access the gateway via SSH.
Remote Data Capture	After this feature is enabled, you can obtain the gateway data via a remote capture tool. The default value is *No*.
Capture RTP	Sets whether to capture RTP. Once this feature is enabled, the RTP package will also be captured by the selected network.
FTP	Sets whether to enable the FTP server, with the default value of *Yes*.
Enable Watchdog	Sets whether to enable the watchdog feature, with the default value of *Yes*.
SYSLOG	Sets whether to enable SYSLOG. It is required to fill in ***SYSLOG Server Address*** and ***SYSLOG Level*** in case SYSLOG is enabled. By default, ***SYSLOG*** is disabled.
Server Address	Sets the SYSLOG server address for log reception.
SYSLOG Level	Sets the SYSLOG level. There are three options: *ERROR*, *WARNING* and *INFO*.
Send CDR	Sets whether to enable the feature of sending CDR. It is required to fill in ***Server Address*** and ***Server Port*** in case Send CDR is enabled. By default, ***Send CDR*** is disabled.
Server Address	The address of the server to receive CDR.
Server Port	The port of the server to receive CDR.
Send Failed Call Record	Once this feature is enabled, the gateway will send the CDR for both successful and unsuccessful calls; otherwise, it will only send the CDR data for successful calls.
Add Hangup Side	Add hangup information to CDR.
Add Lan1,2 IPv4 Address	Add the IP address corresponding to the network port to CDR.
Monitor Self-adaption	Enable the NAT stun between the gateway and the monitor tool. By default, it is disabled.

NTP	Sets whether to enable the NTP time synchronization feature. It is required to fill in ***NTP Server Address***, ***Synchronizing Cycle*** and ***Time Zone*** in case NTP is enabled. By default, ***NTP*** is disabled.
NTP Server Address	Sets the Server address for NTP time synchronization.
Synchronizing Cycle	Sets the cycle for NTP time synchronization.
Daily Restart	Sets whether to restart the gateway regularly every day at the preset ***Restart Time***. By default, this feature is disabled.
Restart Time	Sets the time to restart the gateway regularly.
System Time	The system time. Check the checkbox before ***Modify*** and change the time in the edit box.
Time Zone	The time zone of the gateway.

3.3.4 IP Routing Table

IP Routing Table is used to set the route for the gateway to send the IP packet to the destination network segment. By default, there is no routing table available on the gateway, click ***Add New*** to add them manually.

The table below explains the items shown on the interface.

Item	Description
No.	The number of the routing in routing table.
Destination	The network segment where the IP packet can reach.
Subnet Mask	The subnet mask of the destination network segment.
Network Port	The corresponding network port of the routing.

After configuration, click ***Save*** to save the settings into the gateway or click ***Close*** to cancel the settings.

Click ***Modify*** to modify a routing. The configuration items on the routing table modification interface are the same as those on the ***Add Routing Table*** interface. Note that the item ***No.*** cannot be modified.

To delete a routing, check the checkbox before the corresponding index and click the ***Delete*** button. To clear all routing tables at a time, click the ***Clear All*** button.

3.3.5 Access Control

On the Access Control List interface, once you add a piece of command to ACL, the network flow will be restricted, only the particular devices allowed to visit the gateway and only the data packages on the designated ports be forwarded. For easy viewing, the interface provides a display of iptables information. Click ***Add New*** to add a new piece of command.

Input a piece of command into the Command item and click ***Save*** to save the settings to the gateway. Click ***Close*** to cancel your settings. After that, click ***Apply*** to make the new command valid.

Click ***Modify*** to modify a command. The configuration items on the Access Control Command Modification interface are the same as those on the ***Add Access Control Command*** interface. Note that the item ***Index*** cannot be modified.

To delete an Access Control Command, check the checkbox before the corresponding index and click the ***Delete*** button, and then click the ***Apply*** button to make the deleted command invalid. ***Check All*** means to select all available items on the current page; ***Uncheck All*** means to cancel

all selections on the current page; ***Inverse*** means to uncheck the selected items and check the unselected. To clear all access control commands at a time, click the ***Clear All*** button.

Note: 1, Currently, only the command iptables is supported by the gateway.

2, When you add or modify or delete commands manually, don't forget to click the ***Apply*** button to make your settings valid. However, when the gateway restarts or the configuration is leading-in, you need not click the ***Apply*** button and the commands will get valid automatically.

3.3.6 Firewall

By default, there is no firewall information available on the gateway, click ***Add New*** to add it manually.

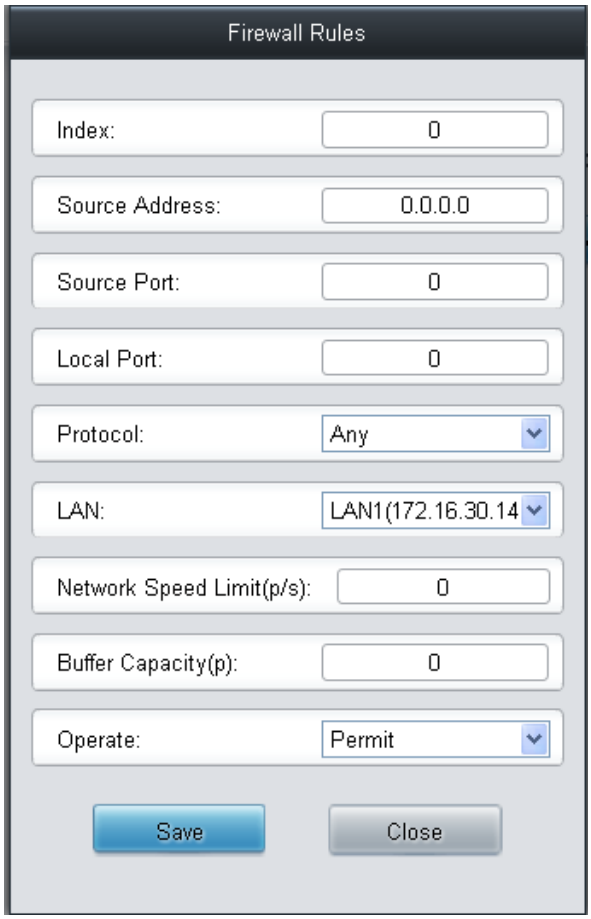

Figure 3-2 Firewall Rules Adding Interface

See below for the configuration items on the interface.

Item	Description
Index	The unique index of a firewall rule, used to specify its priority. The smaller the value, the higher the priority.
Source Address	Set the IP address of the source network or an explicit host name.
Source Port	Set the source UDP/TCP port (remote host) of the packet sent to the gateway.
Local Port	Set the port of the local gateway.
Protocol	Protocol type, including eight options: Any, TCP, UDP, UDPLITE, ICMP, ESP, AH and SCTP.
LAN	Select the network port to which the firewall rule is applied.

Network Speed Limit	Set the expected rate of the network in packs. **Note:** The network packet exceeding the speed limit will be stored in the buffer until the buffer capacity is full, and the overspeed network packet will be discarded.
Buffer Capacity	Set the buffer capacity of the network rate. The default value is 0.
Operate	Set the execution results of firewall rules, including two options: *Permit* and *Prevent*.

After configuration, click ***Save*** to save the settings into the gateway or click ***Close*** to cancel the settings.

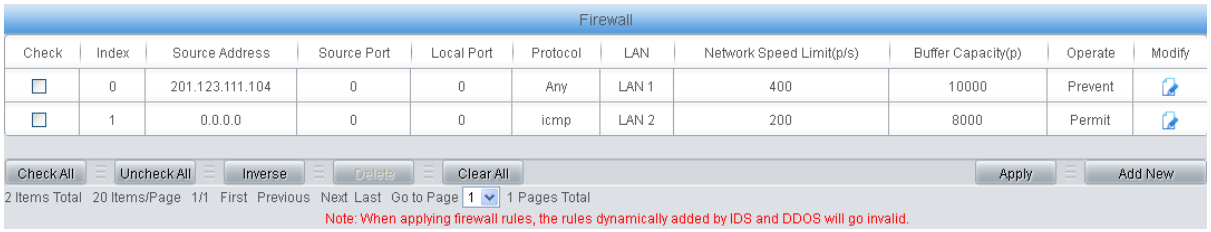

Figure 3-3 Firewall Rules List

Click ***Modify*** to modify a firewall rule. The configuration items on the modification interface are the same as those on the ***Add Firewall Rule*** interface.

To delete a firewall rule, check the checkbox before the corresponding index and click the ***Delete*** button. ***Check All*** means to select all available items on the current page; ***Uncheck All*** means to cancel all selections on the current page; ***Inverse*** means to uncheck the selected items and check the unselected. To clear all rules at a time, click the ***Clear All*** button.

Note: 1. Only after selecting a firewall rule and clicking Apply, the firewall rule will take effect.

2. An IP that is determined to be abnormal by DDOS or IDS, will be added to the temporary blacklist, even if the firewall is set to allow access.

3.3.7 IDS Settings

IDS is used to detect whether the incoming SIP message complies with the protocol specification. For a SIP message that does not conform to the specification, the gateway will add its source IP address to the blacklist. The IDS settings interface is shown in Figure 3-4.

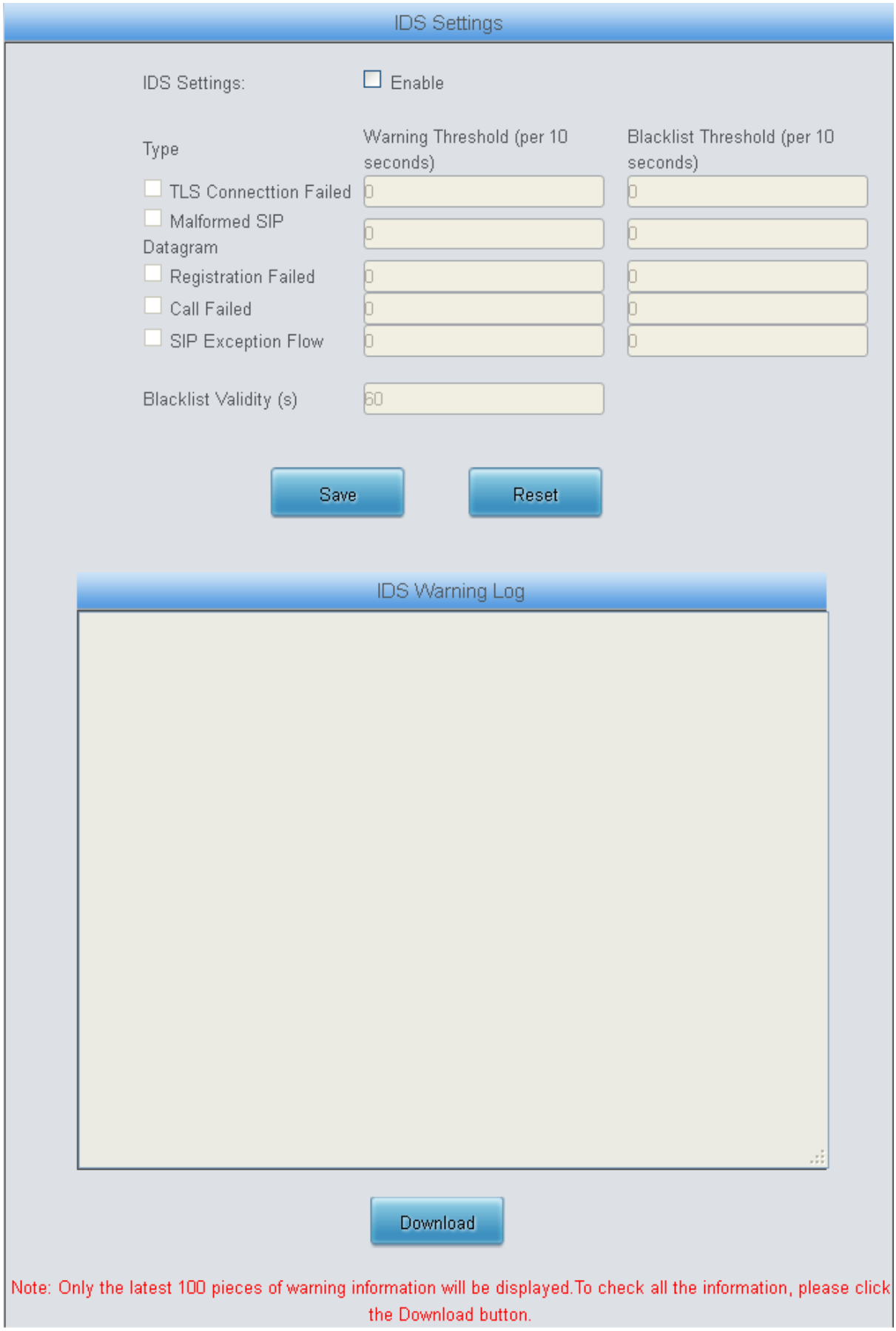

Figure 3-4 IDS Settings Interface

The table below explains the items shown on the interface.

Item	Description
Type	Sets the type for detecting whether the SIP message conforms to the specification or the condition of blacklist, including *TLS Connection Failed*, *Malformed SIP Datagram*, *Registration Failed*, *Call Failed* and *SIP Exception Flow*.
Warning Threshold	Once the detection times of a type reaches the warning threshold, the source IP address contained in the SIP message will be recorded to the IDS warning log.
Blacklist Threshold	Once the detection times of a type reaches the blacklist threshold, the source IP address contained in the SIP message will be recorded to the blacklist.
Blacklist Validity	Set the effective time for the blacklist to work.

After your configuration, click ***Save*** to save the above settings into the gateway, click ***Reset*** to restore the current settings, and click ***Download*** to download the IDS log.

Note: After restarting the service, rebooting the system, upgrading the software or applying the firewall, the temporary blacklist will be cleared.

3.3.8 DDOS Settings

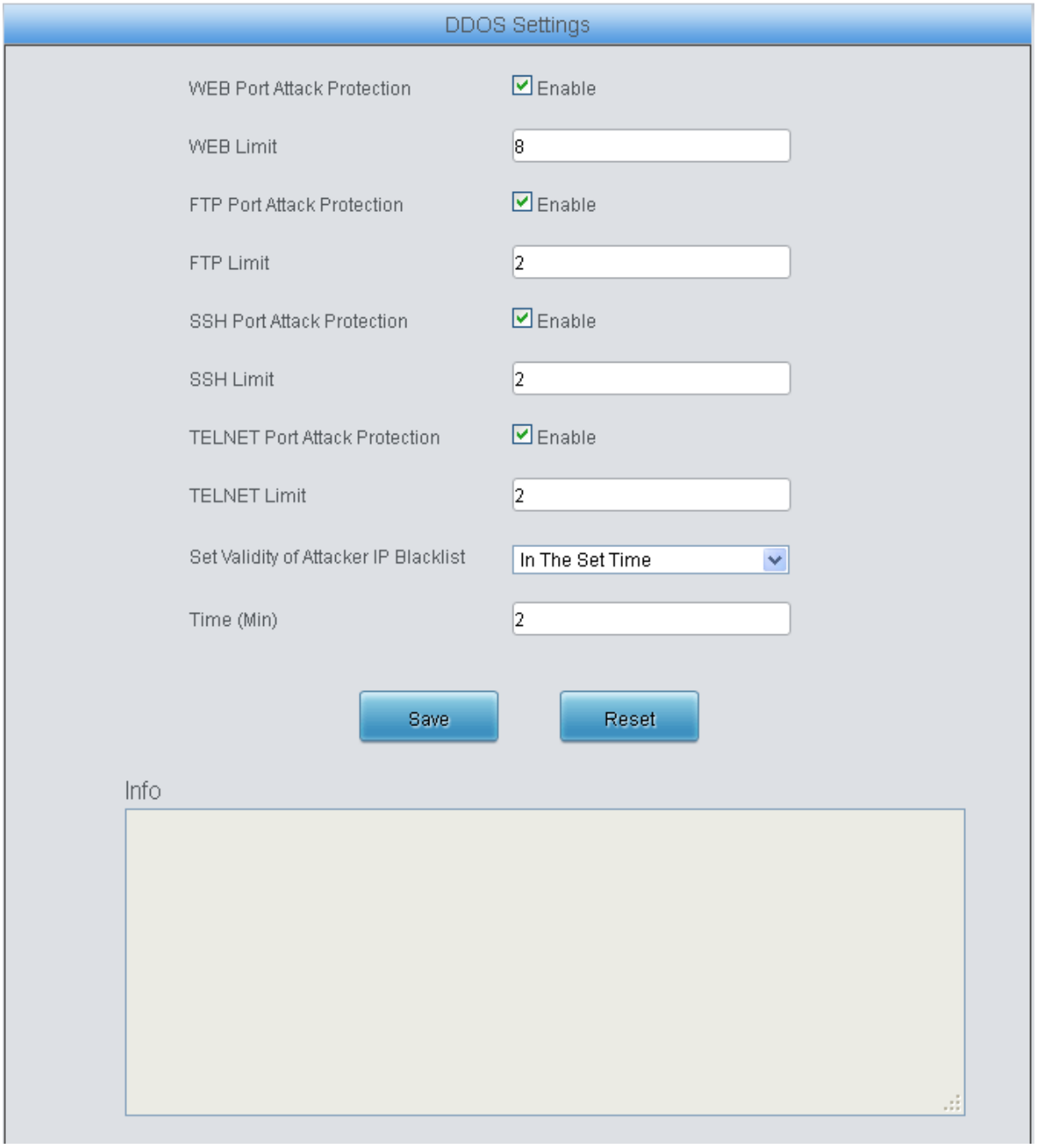

Figure 3-5 DDOS Settings Interface

The DDOS settings interface, as shown in Figure 3-5, can set the defense feature of some ports against DDOS attacks. The table below explains the items shown on the above interface.

Item	Description
WEB Port Attack Protection	When this feature is enabled, the WEB port will have the ability to block DDOS attacks.
WEB Limit	When the same IP address accesses the gateway through WEB, it will be forbidden to log in once the times exceed this set value (the number of access processes is /5).

FTP Port Attack Protection	When this feature is enabled, the FTP port will have the ability to block DDOS attacks.
FTP Limit	When the same IP address accesses the gateway through FTP, it will be forbidden to log in once the times exceed this set value (equal to the number of access processes).
SSH Port Attack Protection	When this feature is enabled, the SSH port will have the ability to block DDOS attacks.
SSH Limit	When the same IP address accesses the gateway through SSH, it will be forbidden to log in once the times exceed this set value (equal to the number of access processes).
TELNET Port Attack Protection	When this feature is enabled, the TELNET port will have the ability to block DDOS attacks.
TELNET Limit	When the same IP address accesses the gateway through TELNET, it will be forbidden to log in once the times exceed this set value (equal to the number of access processes).
Set Validity of Attacker IP Blacklist	Sets the effective time of the attack blacklist, including two options *Forever* and *In the Set Time*.
Time	Sets the effective time for the blacklist to work.

After your configuration, click ***Save*** to save the above settings into the gateway, or click ***Reset*** to restore the current settings.

Note: After rebooting the system, upgrading the software or applying the firewall, the temporary blacklist will be cleared.

3.3.9 Configuration File

Via the Configuration File interface, you can check and modify configuration files about the gateway, including SMGConfig.ini, ShConfig.ini and hosts. Configurations about the gateway server, such as route rules, number manipulation, number filter and so on, are included in SMGConfig.ini; configurations about the board are included in ShConfig.ini; and hosts is the system file relating a domain name and its corresponding IP address. You can modify these configurations on the interface directly, and then click ***Save*** to save the above settings into the gateway or click ***Reset*** to restore the configurations.

3.3.10 Signaling Capture

On the Signaling Capture interface, Data Capture is used to capture data on the network interface you choose. Click ***Start*** to start capturing data (up to 800M) on the corresponding network interface. At present SIP and SysLog are supported for you to choose. If Syslog is selected, you need enter the Syslog destination address to send Syslog to wherever required. Click ***Stop*** to stop data capture and download the captured packets.

Two-way Recording is used to set the channel group and the channel number for recording. Click ***Start*** to start recording the corresponding channel in the specified channel group (maximum consecutively recording time is 1 minute). Click ***Stop*** to stop recording and download the recorded data. Once the option Capture RTP is ticked, you are required to input the calling number of the RTP to be captured.

Click ***Clean Data*** to clean all the recording files and captured packages. Click ***Download Log*** to download such logs as core files, configuration files, error information and so on.

3.3.11 PING Test

Via the Ping Test interface, a Ping test can be initiated from the gateway on a designated IP address to check the connection status between them. The table below explains the configuration items shown on the interface.

Item	Description
Source IP Address	Source IP address where the Ping test is initiated.
Destination Address	Destination IP address on which the Ping test is executed.
Ping Count	The number of times that the Ping test should be executed. Range of value: 1~100.
Package Length	Length of a data package used in the Ping test. Range of value: 56~1024 bytes.
Info	The information returned during the Ping test, helping you to learn the network connection status between the gateway and the destination address.

After configuration, click ***Start*** to execute the Ping test; click ***End*** to terminate it immediately.

3.3.12 TRACERT Test

Via the Tracert Test interface, a Tracert test can be initiated from the gateway on a designated IP address to check the routing status between them. The table below explains the configuration items shown on the interface.

Item	Description
Source IP Address	Source IP address where the Tracert test is initiated.
Destination Address	Destination IP address on which the Tracert test is executed.
Maximum Jumps	Maximum number of jumps between the gateway and the destination address, which can be returned in the Tracert test. Range of value: 1~255.
Info	The information returned during the Tracert test, helping you to learn the detailed information about the jumps between the gateway and the destination address.

After configuration, click ***Start*** to execute the Tracert test; click ***End*** to terminate it immediately.

3.3.13 Modification Record

The Modification Record interface is used to check the modification record on the web configuration. Click ***Check*** and the modification record will be shown on the dialog box. Click ***Download*** to download the record file.

3.3.14 Backup & Upload

On the Backup and Upload interface, to back up data to your PC, you shall first choose the file in the pull-down list and then click ***Backup*** to start; to upload a file to the gateway, you shall first choose the file type in the pull-down list, then select it via ***Browse…***, and at last click ***Upload***. The gateway will automatically apply the uploaded data to overwrite the current configurations.

3.3.15 Factory Reset

On the Factory Reset interface, click ***Reset*** to restore all configurations on the gateway to factory settings.

3.3.16 Upgrade

On the upgrade interface, you can upgrade the WEB, gateway service, kernel and firmware to new versions. Select the upgrade package "*.tar.gz" via ***Browse…*** and click ***Update*** (The gateway will do MD5 verification before upgrading and will not start to upgrade until it passes the verification). Wait for a while and the gateway will finish the upgrade automatically. Note that clicking ***Reset*** can only delete the selected update file but not cancel the operation of ***Update***.

3.3.17 Account Manage

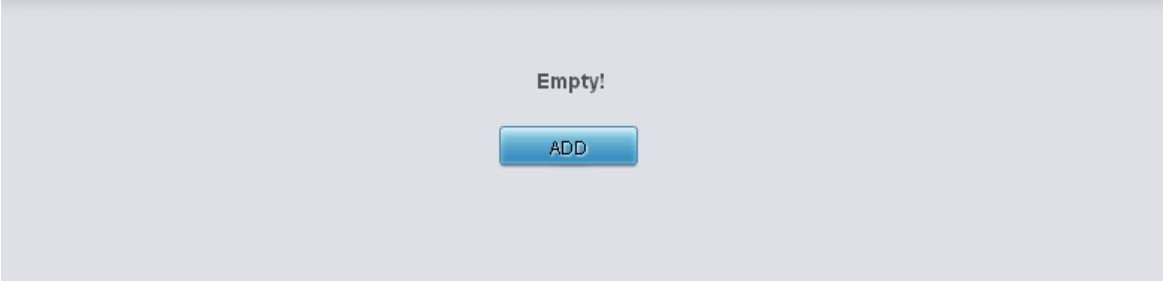

Figure 3-6 Account Management Interface

See Figure 3-6 for the Account Management interface. By default, there is no user information available on the gateway, click ***Add*** to add a piece of information.

Figure 3-7 User Information Adding Interface

The table below explains the configuration items shown on the interface.

Item	Description
Index	The unique index of each user information, starting from 0 and supporting up to 64 pieces of user information to add.
User Name/Password	User name and password for WEB login. Only numbers, letters and underscores are supported.
Authority	Operation rights, including two options *Read* and *Read/Write*.

After configuration, click ***Save*** to save the settings into the gateway or click ***Close*** to cancel the settings. See Figure 3-8 for the user information list.

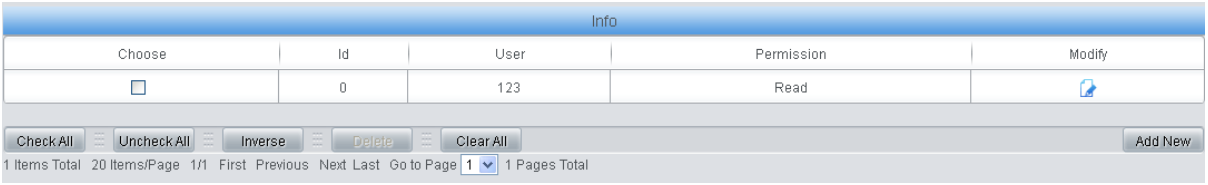

Figure 3-8 User Information List

Click ***Modify*** in Figure 3-8 to modify a piece of user information. The configuration items on the user information modification interface are the same as those on the ***User Information Adding*** interface. Note that the item ***Index*** cannot be modified.

To delete a piece of user information, check the checkbox before the corresponding index in Figure 3-9 and click the ***Delete*** button. ***Check All*** means to select all available items on the current page; ***Uncheck All*** means to cancel all selections on the current page; ***Inverse*** means to uncheck the selected items and check the unselected. To clear all user information at a time, click the ***Clear All*** button.

3.3.18 Change Password

On the Password Changing interface you can change username and password of the gateway. Enter the current password, the new username and password, and then confirm the new password. After configuration, click ***Save*** to apply the new username and password or click ***Reset*** to restore the configurations. After changing the username and password, you are required to log in again.

3.3.19 Device Lock

On the Device Lock Configuration interface, when you select one or more than one conditions to lock the gateway, the configurations of the gateway related to the selected conditions will be all locked. That is, to modify any one of those configurations, you are required to input the lock password. Click ***Lock*** after setting and the device lock interface will be locked. To unlock the interface, enter your password (just the lock password) and click the ***Unlock*** button.

3.3.20 Restart

On the Restart interface, click ***Restart*** on the service restart interface to restart the gateway service or click ***Restart*** on the system restart interface to restart the whole gateway system.

Appendix A Technical Specifications

Dimensions

440×44×267 mm^3

Weight

About 3.1 kg

Environment

Operating temperature: 0℃—40℃

Storage temperature: -20℃—85℃

Humidity: 8%— 90% non-condensing

Storage humidity: 8%— 90% non-condensing

LAN

Amount: 2 (10/100/1000 BASE-TX (RJ-45))

Self-adaptive bandwidth supported

Auto MDI/MDIX supported

Console Port

Amount: 1 (RS-232)

Baud rate: 115200bps

Connector: RJ45 （See Hardware Description for signal definition）

Data bits: 8 bits

Stop bit: 1 bit

Parity unsupported

Flow control unsupported

Note: Follow the above settings to configure the console port; or it may work abnormally.

Power Requirements

Input power: 100~240V AC

Maximum power consumption: ≤22W

Signaling & Protocol

SIP signaling: SIP V1.0/2.0, RFC3261

Audio Encoding & Decoding

G.711A	*64 kbps*
G.711U	*64 kbps*
G.729	*8 kbps*
G723	*5.3/6.3 kbps*
G722	*64 kbps*
AMR-NB	*4.75/5.15/5.90/6.70/7.40/7.95/10.20/12.20 kbps*
iLBC	*15.2 kbps*
SILK(16K)	*20 kbps*
OPUS(16K)	*20 kbps*
SILK(8K)	*20 kbps*
OPUS(8K)	*20 kbps*

Sampling Rate

8kHz

Safety

Lightning resistance: Level 4

Appendix B Troubleshooting

1. What to do if I forget the IP address of the SR500 gateway?

Long press the Reset button on the gateway to restore to factory settings. Thus the IP address will be restored to its default value:

LAN1: 192.168.1.101

LAN2: 192.168.0.101

2. In what cases can I conclude that the SR500 gateway is abnormal and turn to Synway's technicians for help?

a) During runtime, the run indicator does not flash or the alarm indicator lights up or flashes, and such error still exists even after you restart the device or restore it to factory settings.

b) Voice problems occur during call conversation, such as that one party or both parties cannot hear the voice or the voice quality is unacceptable.

Other problems such as abnormal channel status, inaccessible calls, failed registrations and incorrect numbers are probably caused by configuration errors. We suggest you refer to Chapter 3 WEB Configuration for further examination. If you still cannot figure out or solve your problems, please feel free to contact our technicians.

3. What to do if I cannot enter the WEB interface of the SR500 gateway after login?

This problem may happen on some browsers. To settle it, follow the instructions here to configure your browser. Enter 'Tools > Internet Options >Security Tab', and add the current IP address of the gateway into 'Trusted Sites'. If you change the IP address of the gateway, add your new IP address into the above settings.

Appendix C Technical/sales Support

Thank you for choosing Synway. Please contact us should you have any inquiry regarding our products. We shall do our best to help you.

Headquarters

Synway Information Engineering Co., Ltd

http://www.synway.net/

9F, Synway D&R Center, No.3756, Nanhuan Road, Binjiang District, Hangzhou, P.R.China, 310053

Tel: +86-571-88860561

Fax: +86-571-88850923

Wechat QR Code: Scan the QR code below to add us on Wechat.

Technical Support

Tel: +86-571-88864579

Mobile: +86-18905817070

Email: techsupport@sanhuid.com

Email: techsupport@synway.net

MSN: synway.support@hotmail.com

Sales Department

Tel: +86-571-88860561

Tel: +86-571-88864579

Fax: +86-571-88850923

Email: sales@synway.net