New Rock Technologies, Inc.

SX1000 Enterprise Session Border Controller (SBC)

Administrator Manual

http://www.newrocktech.com
Tel: +86 21-61202700
Fax: +86 21-61202704

Document No. : AS0-E002-P
Document version: 201308

Contents

Contents of Figure

Contents of Table

1 Equipment Structure

1.1 Front Panel

Figure 1-1 SX1000 front panel

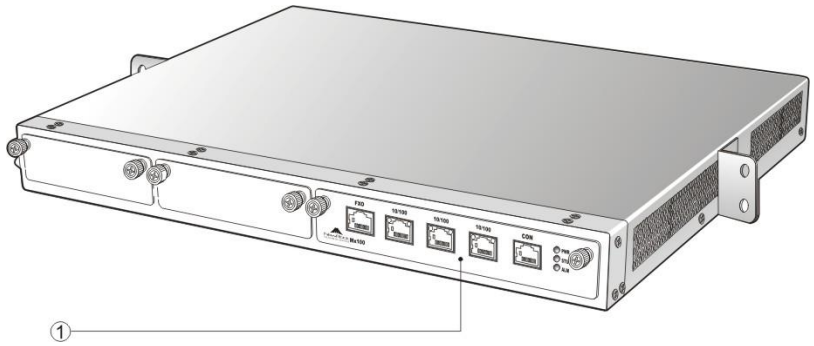


Table 1-1 Description of SX1000 front panel

#	Description
①	Main control module. It offers three 10/100M Ethernet port and one configuration interface (CON). Note: DO NOT plug or remove the main control module when the device is powered on.

Table 1-2 Indicators of SX1000

Mark	Function	Status	Description
PWR	Power Indication	Green	Power on.
		Off	Power off.
STU	Status Indication	Off	System locked and inactive.
		Green Flash	Normal operation.
		Constant Red	System in the process of powerup and not in the normal normal operation mode.
		Red Flash	System in a diagnostic mode and able to execute limited operation.
ALM	Alarm Indication	Green	No alarms.
		Red Flash	New alarms occurred but not confirmed.
		Red	Alarms existed and all alarm information confirmed.

Figure 1-2 SX1000 back panel

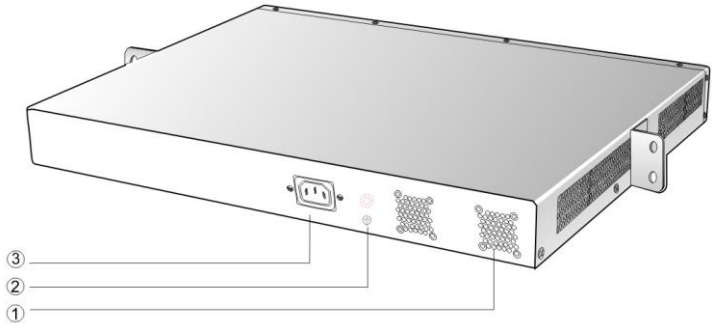


Table 1-3 Description of SX1000 back panel

#	Description
①	Two cooling fans
②	Ground pole
③	AC power socket, 100-240 VAC voltage input.

1.2 Main Control Module

SX1000 Main Control Module is equipped with advanced framework and technology. Its main features include: high performance processors for management and signaling processing and DSP sub module for voice processing. The Main Control Module provides necessary interfaces connecting peripheral devices and internal interface modules.

Figure 1-3 Main control module physical view

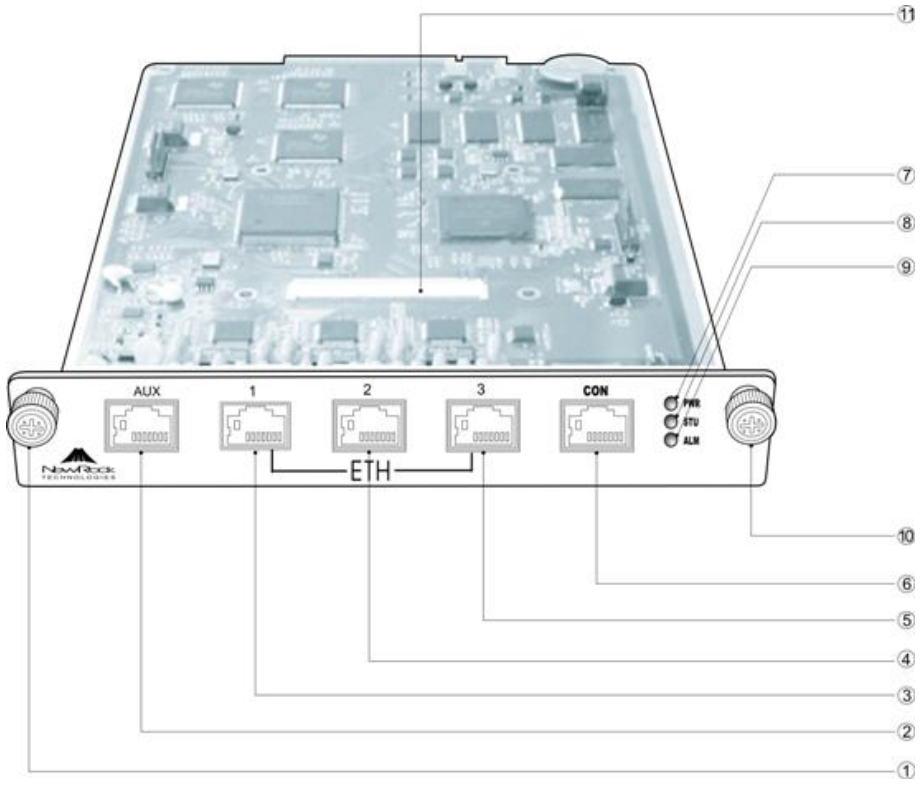


Table 1-4 Description of main control module

#	Description	#	Description
①	Thumb Screw	②	AUX port（currently not supported）
③	Ethernet Port 1	④	Ethernet Port 2
⑤	Ethernet Port 3	⑥	Console Port (CON)
⑦	PWR LED	⑧	STU LED
⑨	ALM LED	⑩	Thumb Screw
⑪	DSPDC Connector (advanced voice processing technology)		

Note

The main console module can be secured by turning the screw clockwise. Turn screws the other way to pull the main console module out when the device is powered off.

1.3 Ethernet Port

There are three 10/100M Ethernet ports on the SX1000 main control module, RJ45 with status LED. Table 1-10 shows the pin assignment of those Ethernet connectors and LED status specification.

Table 1-5 Ethernet port pin assignment and status LED specification

RJ45 Pin-out				LED Status	
1	2	3	6	Yellow	Green
TX+	TX-	RX+	RX-	Connected	Live

Note

- If only one Ethernet port is to be used, select a random one to configure;
- If two or three Ethernet ports are to be used, configure them to different IP addresses. One is configured to logical IP address, while the others are transforwarded to Ethernet ports of logical address by signaling to accomplish communication.

1.4 CON (Console) Port

SX1000 supports configuration through a console port (CON) of RJ45 connector. Table1-12 shows the connector interface scheme of RJ45.

Table 1-6 Console port pin assignment of RJ45

RJ45 Connector Pin No.	1	2	3	4	5	6	7	8
Pin Description	NC	NC	TXD	GND	GND	RXD	NC	NC
DB9 Connector Pin No.			2		5	3		
DB25 Connector Pin No.			3		7	2		

The console port is used for local management and testing. Computers can be connected to SX1000 by linking the RS232 port to MX100-AG console port. SX1000 uses three wires on the console port: one TXD (send), one RXD (receive), and one GND (ground).

SX1000 is shipped with a standard RJ45 to DB9 adapter.

Table 1-7 Console port specification

Attribute	Description
Connector Type	RJ45
Port Number	1
Interface Type	RS232
Baud Rate	115200
Data Bits	8
Parity Check	No
Stop Bit	1
Flow Control	No

2 Parameter Settings

Note

There is no license control for SX1000.

2.1 Login

Enter the IP address of SX1000 in the address bar of the browser. Note that the factory default of ETH1 address is 192.168.2.240.

Figure 2-1 Login interface

Login users are classified into **administrator** and **operator**. The default password is as follows. Default Administrator Passwords (lowercase letters required): sx1000. Default Operator Password: operator. The password is shown in a cipher for safety.

- The administrator can browse and modify all configuration parameters, and modify login passwords.
- The operator can browse and modify part of configuration parameters.

The device allows multiple users to login:

- The administrator has permission for modification and the operator has permission for browsing;
- When multiple users with same level of permission log in, the first has permission for modification, while the others only have permission for browsing.

Note

- The system will confirm timeout if users do not conduct any operation within 10 minutes after login. They are required to login again for continuing operations.
- Upon completion of configuration, click **Logout** to return to the login page, so as not to affect the login permission of other users.

2.2 Buttons Used on Management Interface

Submit Button: Submit configuration information. Users click **Submit** after completion of parameter configuration. A success prompt will appear if configuration information is accepted by the system; if a "The configuration takes effect after the system is restarted" dialog box appears, it means that the parameters are valid only after system restarts; it is recommended that users press the **Restart** on the *Tool* page to validate the configuration after changing all parameters to be modified.

2.3 Network Configuration

ETH1 is the factory default Ethernet port, and ETH2 or ETH3 can be enabled according to the application. Fill in the network parameters, including IP address, netmask and gateway IP address, and click Submit to save the configuration. When more than one Ethernet ports are used, the IP addresses are not allowed in the same network segment.

If the gateway address is configured for all the three Ethernet interfaces, the IP address of Ethernet interface 2 is the default gateway.

If Ethernet interface 2 is not used or configured with the gateway, the IP address of Ethernet interface 3 is the default gateway. If only Ethernet interface 1 is used, the IP address of Ethernet interface 1 is the default gateway.

Note

In the scenario in which multiple Ethernet ports are used, each of the Ethernet ports must be in a separate subnet.

After login, click **Network** to launch the configuration interface.

Figure 2-2 Network configuration interface

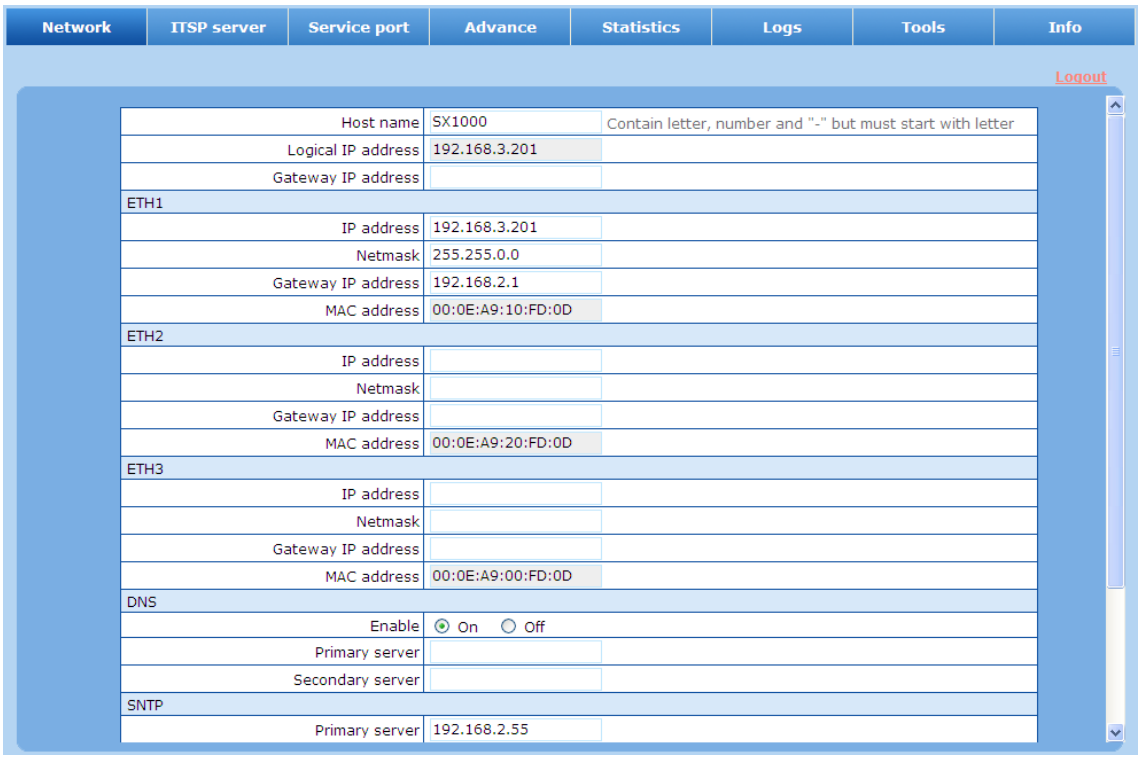


Table 2-1 Network configuration parameters

Name	Description
Hostname	The default value is SX1000. Users can set a different name for each device to distinguish from each other according to the deployment plan. A host name can be a maximum of 48 characters, either letters (A-Z or a a-z), numbers (0-9) and minus sigh (-). It may not be null or space, and it must start with a letter.
Logical IP address	Display the actual IP address in use.
Gateway IP address	Default IP address
Eth 1	Fill in the IP address, subnet mask, gateway IP address, MAC address of Eth 1.
Eth 2	Fill in the IP address, subnet mask, gateway IP address, MAC address of Eth 2.
Eth 3	Fill in the IP address, subnet mask, gateway IP address, MAC address of Eth 3.
DNS	
Enable	Activate DNS service.
Primary server	If DNS service is activated, the network IP address of preferred DNS server must be entered, and there is no default value.
Secondary server	If DNS service is activated, the network IP address of standby DNS server can be entered here. It is optional and there is no default value.
SNTP	
Primary server	Enter the IP address of preferred time server here. This parameter must be set due to no default value.
Secondary server	Enter the IP address of standby time server here. This parameter must be set due to no default value.
Timeout	If the server is not located within the time allowed, SX1000 will try to locate it again. Unit: minute

Name	Description
Interval	Enter the time interval at which SX1000 will synchronize its time with the time server. Unit: minute
Time zone	Select a time zone, and the parameter values include: • (GMT-11:00) Midway Island • (GMT-10:00) Honolulu. Hawaii • (GMT-09:00) Anchorage, Alaska • (GMT-08:00) Tijuana • (GMT-06:00) Denver • (GMT-06:00) Mexico City • (GMT-05:00) Indianapolis • (GMT-04:00) Glace_Bay • (GMT-04:00) South Georgia • (GMT-03:30) Newfoundland • (GMT-03:00) Buenos Aires • (GMT-02:00) Cape_Verde • (GMT) London • (GMT+01:00) Amsterdam • (GMT+02:00) Cairo • (GMT+03:00) Moscow • (GMT+03:30) Teheran • (GMT+04:00) Muscat • (GMT+04:30) Kabul • (GMT+05:30) Calcutta • (GMT+05:00) Karachi • (GMT+06:00) Almaty • (GMT+07:00) Bangkok • (GMT+08:00) Beijing • (GMT+09:00) Tokyo • (GMT+10:00) Canberra • (GMT+10:00) Adelaide • (GMT+11:00) Magadan • (GMT+12:00) Auckland

2.4 ITSP Server Configuration

Click **ITSP** and enter the configuration interface of SIP proxy. Up to 5 SIP proxies can be added. Each proxy starts with an ID and followed by the IP address of the proxy including the address and the UDP port of receiving messages, e.g. 192.168.1.20:5060. Select **Yes** for ***Sending response to rport*** if SX1000 needs to send response messages to the sending port of the proxy. Otherwise, select **No**.

Figure 2-3 ITSP server configuration interface

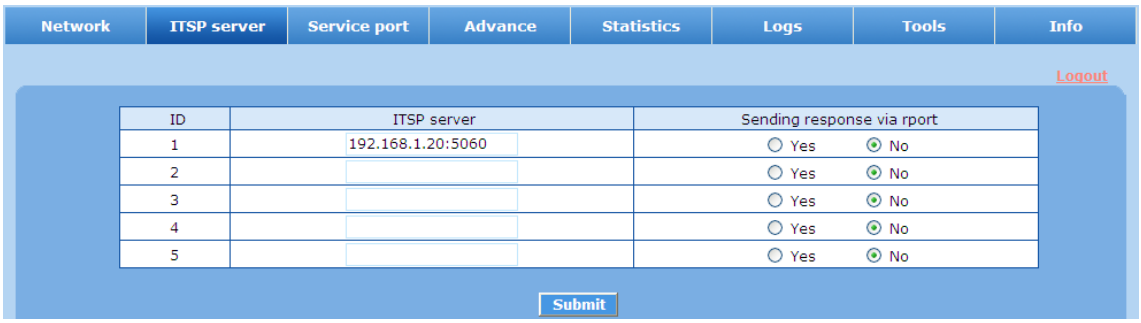


Table 2-2 ITSP server configuration parameter

Name	Description
ITSP server 1-5	The IP addresses and port numbers of ITSP servers, separated by ":".

Note

- This parameter cannot be configured as localhost, 127.0.0.1, 0.0.0.0 or the IP address of SX1000.
- The port number of ITSP server also must be filled in.
- When this device is deployed with SoftCo based solution, it is recommended to fill in No to avoid the normal operation of the device.
- If no IP address of all the three Ethernet interfaces on SX1000 is in the same network segment as that of the softswitch, SX1000 forwards registration messages through a logical IP address. The logical IP address can be queried in the Network tag of the GUI and cannot be changed. By default, the IP address of Ethernet interface 1 is used as the logical IP address. If Ethernet interface 1 is not configured, the IP address of Ethernet interface 3 will be used as the logical IP address. If only the IP address of Ethernet interface 2 is configured, the IP address of Ethernet interface 2 is used as the logical IP address.

2.5 Service Port Configuration

The service port is used to receive the SIP messages from terminals, which will be processed and redirect to the ITSP softswitch associated to the port.

Up to 5 service ports can be configured on SX1000, each associated with a primary softswitch and its backup softswitches.

Up to 2 backup softswtiches can be associated with a service port, Backup 1 and Backup 2. When heartbeat function on SX1000 is enabled, the system will monitor the availability of the softswitch. The system will failover to the backup softswitch once the primary softswitch becomes not accessible, and will be failback when the primary recovers.

The messages received from a service port can be encrypted if it is required. The encryption can be applied to media streams and/ or the SIP messages, and the factory default is no encryption. When the encryption is selected, SX1000 will perform decryption to the received messages from terminals before they are redirected to the softswitch; similarly, SX1000 will perform encryption to the messages from the softswitch before they are sent to the terminals.

There are 3 encryption schemes which can be selected to apply to the media streams, including

- RTP: perform encryption to the entire RTP packets;
- RTP Header: perform encryption only to the headers of RTP packets;
- RTP Body: perform encryption only to the bodies of RTP packets.

Encryption key may be needed for some encryption methods, and the key used should be identical on both SX1000 and the terminals.

When TLS encryption method is selected, SRTP will be used to encrypt/decrypt RTP packets. SSL certificate related setting should be configured.

Three Eth ports of SX1000: Eth 1, Eth 2, Eth 3. Different parameters should be applied according to different Eth ports. Users can configure corresponding configuration of each Eth port. Take "Eth 1" for example.

After login, click **Service port** > **Eth 1** to launch the configuration interface.

Figure 2-4 Service port configuration interface

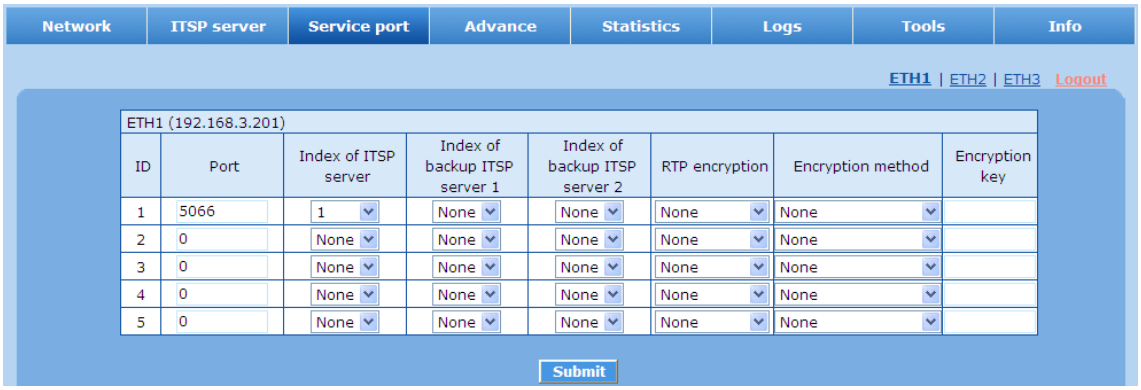


Table 2-3 Service port configuration parameter

Name	Description
Eth 1 (IP address)	Display IP address of Eth 1 which configured at **network** parameter configuration. (Read only)
Port	To configure ports of signaling encryption & non-encryption.
Index of ITSP server	To configure ITSP numbers of signaling encryption & non-encryption. ITSP No. 1~5 are supported right now. (auto-identification, read only).
RTP encrption	Four ways: None; RTP(RTP Header & RTP Body); RTP Header (RTP/Header Document); RTP Body (RTP package)

Name	Description
Encryption method	Eight ways: • None: non-encryption • TLS • TCP Not Encrypted: package signaling (RTP) by TCP Protocol; non-encryption • TCP Encrypted: package signaling (RTP) by TCP Protocol; encryption used • UDP Not Encrypted: package signaling (RTP) by UDP Protocol; non-encryption • UDP Encrypted: package signaling (RTP) by UDP Protocol; encryption used • Using Keyword • Using Keyword2 • Encrypt 14
Encryption key	Obtain from service provider. Not applied to UDP Encrypted.

2.6 Advanced Configuration

2.6.1 System

After login, click **Advance** > **System**.

Figure 2-5 Interface of sysem advanced configuration

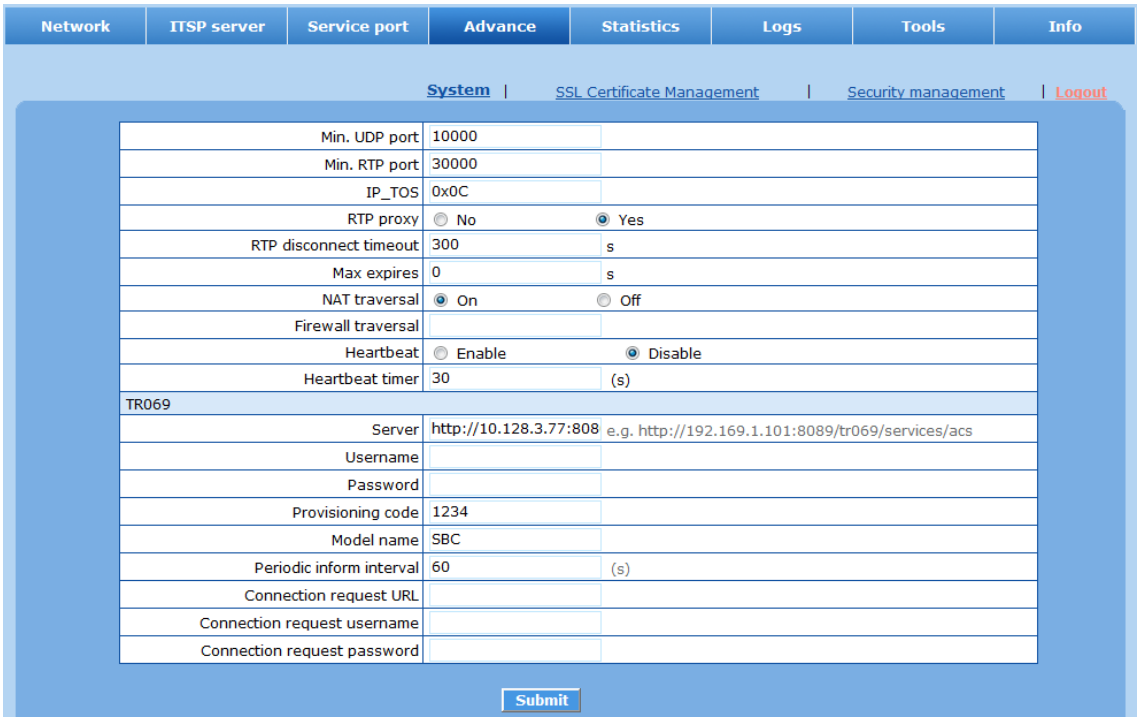


Table 2-4 Parameters of system advanced configuration

Name	Description
Min. UDP port	Above 10000 (advised).
Min. RTP port	Above 30000 (advised).

Name	Description
IP_TOS	To define QoS of different levels. Default value: 0x00. Eg: TOS=0xB8 indicats that the previous level is 5. Low time delay & high throughput is required. No requirements for the stability.
RTP proxy	To configure whether RTP is transmitted by SX1000.
RTP disconnect timeout	Shut down RTP if there's no RTP during configuration time interval. Unit: second; virtual value: 180-1200 seconds.
Maximum registration period	The maximum period (in second) allowed for terminal registration. The default value is 0, which allows the terminal to register according to its original registration period, • If the original registration period is less than the maximum registration period, the terminal registers according to its original period. • If the original registration period is longer than the maximum registration period, the terminal registers according to the maximum registration period.
NAT traversal	• On: gateway IP address by Via、Contact revised into IP address of SX1000. • Off: non-revise.
Firewall address	When SBC device is exclusive to the firewall and is deployed cross the firewall, IP address of the firewall must be filled in. Note: Need to configure DMZ on the firewall for SX1000.
Heartbeat	The heartbeat for detecting the status of SoftCo.
Heartbeat timer	The period for repeating the heartbeat.
TR069	
Server	Enter the IP address of TR069 network management system.
Username	Enter the username of the adninstrator.
Password	Enter the password of the administrator.
Provisioning code	Only digits and characters are permitted.
Model name	The model name of SX1000. The default is SBC.
Periodic inform interval	In second.
Connection request URL	HTTP URL for an ACS to make a Connection Request notification to SX1000. In the form: http://host:port/path
Connection request username	Username used to authenticate an ACS making a Connection Request to the SX1000.
Connection request password	Password used to authenticate an ACS making a Connection Request to SX1000.

2.6.2 SSL Certificate Management

After login, click **Advance** > **SSL Certificate Management**.

Table 2-5 SSL certificate management interface

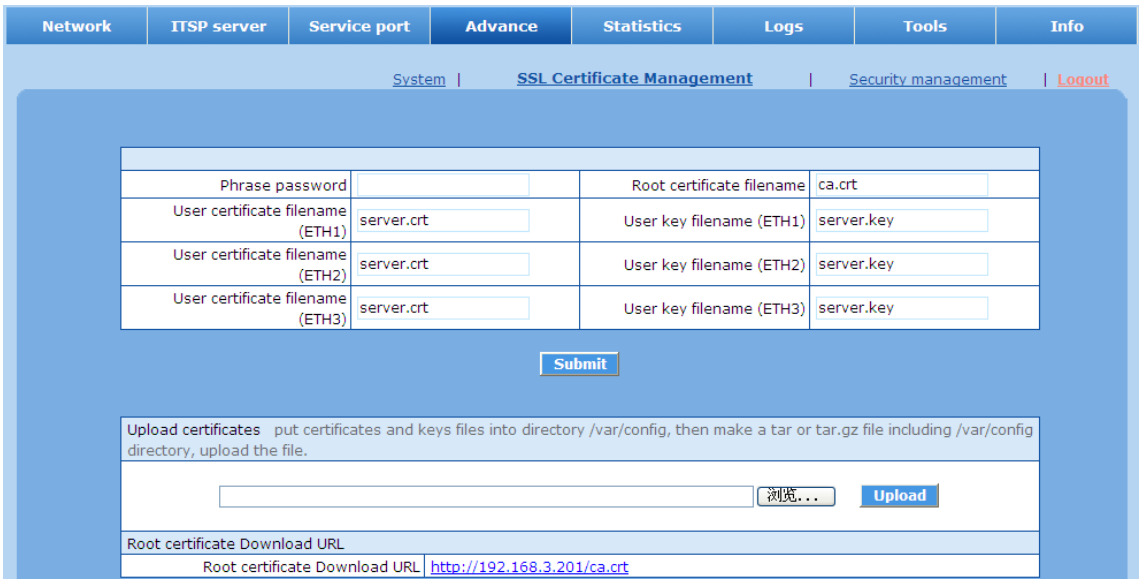


Table 2-6 SSL certificate management configuration parameters

Name	Description
Phrase password	The password used to generate SSL CA certificate.
Root certificate filename	The name of the file which contains the root CA certificate.
User certificate filename (ETH1/2/3)	The name of the file which contains the custom CA certificate for ETH1/2/3.
User key filename (ETH1/2/3)	The name of the file which contains the custom private key for ETH1/2/3.
Upload certificates	Upload the certificate.
URL for root certificate download	The address for downloading root certificate.

2.6.3 Security Management

Telnet service can be disabled or enabled on the **Advance** > **Security** interface. When this service is disabled, telnet is not allowed to logon to SX1000.

IP Table can be setup to filter out the packets from unwanted sources.

After login, click **Advance** > **Security management**.

Figure 2-6 Security management configuration interface

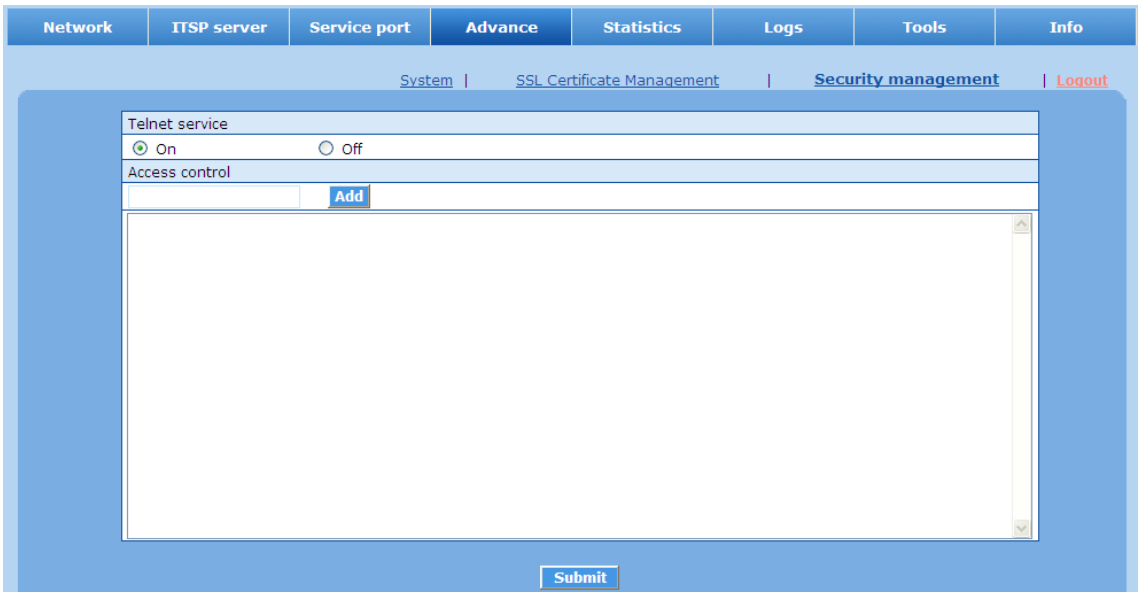


Table 2-7 Security management configuration parameters

Name	Description
Telnet service	Only HTTP port available Users can only login, administrate and maintain the device by web. And only authorized IP address can get accessed. TELNET service is optional.
Access control	Eg: /var/bin/iptables -A OUTPUT -d 192.168.250.230 -p icmp -j DROP This message won't Ping us to the host computer of IP address which is 192.168.250.230. But it has no influence on other host computers. User may change the specified IP address to prevent Pinging corresponding host computers. /var/bin/iptables -A INPUT -p tcp --dport 80 -s 192.168.250.230 -j DROP This message won't access host computer of IP address which is 192.168.250.230 to SX1000 by http, but it won't have influence on other host computers. User may change the specified IP address to prevent corresponding host computers to access SX1000。 iptables –F all existed rules eliminated

2.7 Call Status and Statistics

2.7.1 Online Devices

After login, click **Statistics** > **Online Devices** to launch the configuration interface. All Web login user information (IP address & level) and information of online gateways can be seen.

Figure 2-7 Online devices configuration interface

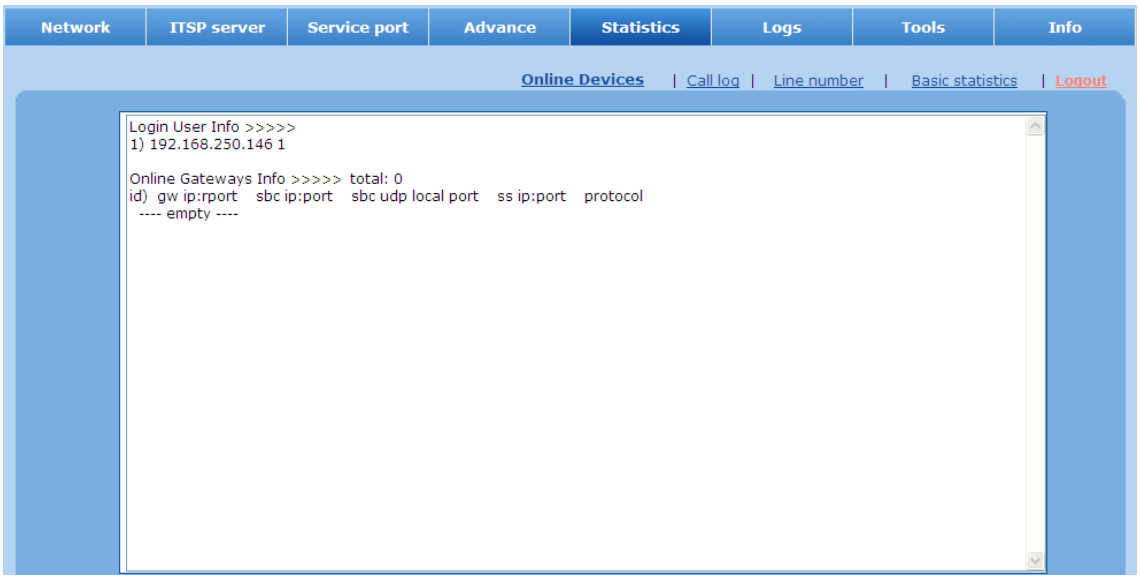


Table 2-8 Parameters of system status

Title	Explanation
Login User Info	Multiple login IP address will be shown. The number 1 or 3 follows IP address. The number 1 indicates operator login. The first login user's IP address is followed by 1. Others are followed by 3. Login level of 2 can be seen as operator. Login level of 2 or 3 cannot modify the configuration.
Online Gateways Info	• total • id • gw ip:rport • sbc ip:port • sbc udp local port • ss sip:port • protocol: MGCP; SIP

2.7.2 Call Log

After login, click **Statistics** > **Call Log**.

Figure 2-8 Call log interface

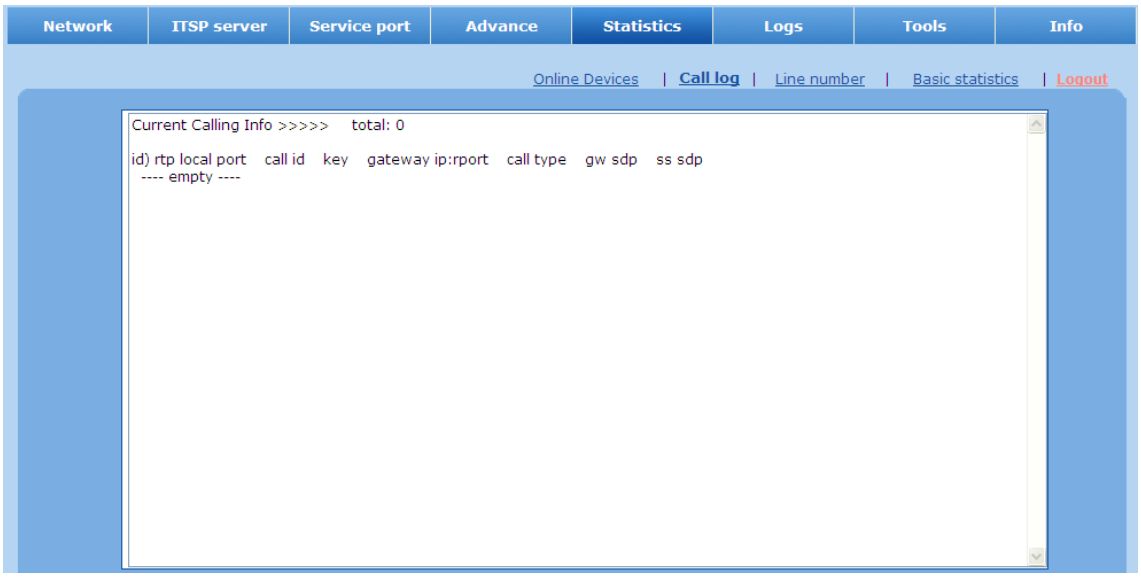


Table 2-9 Call log configuration parameters

Name	Description
Current RTP Callog Info	• Total: The number of established calls • rtp local port: Local RTP port • gateway ip:rport: The gateway IP address and port number • call type: There are two types of call, incoming for inbound calls and outgoing for outbound calls • gw sdp: The SDP addresses of online terminals • ss sdp: The SDP address of ITSP server

Note

- If **Advance > System > RTP control** Interface is set as **no**, there's no information on the **Call Log** Interface.
- If **Advance > System > RTP control** Interface is set as always, information will be displayed on the **Call Log** Interface.

2.7.3 Line Number

After login, click **Statistics** > **Line number** to launch the configuration interface.

Figure 2-9 Line number configuration interface

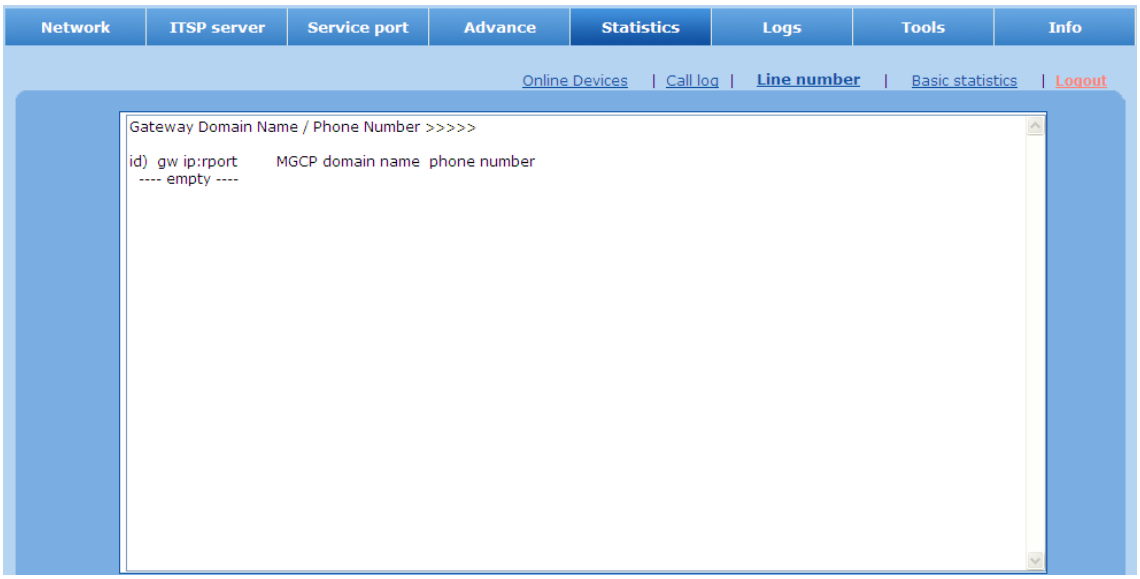


Table 2-10 Line number configuration parameters

Name	Description
Line number	• Id: The ID of a terminal • gw ip:rport: The address and port number of a terminal • phone number: The phone number associated with the terminal

2.7.4 Basic Statistics

After login, click **Statistics** > **Basic** statistics to launch the configuration interface.

Figure 2-10 Basic statistics interface

2.8 Log Management

2.8.1 Managing Log

After login, click **Logs** > **Managing Log**. Log files can be downloaded through this interface.

Figure 2-11 Interface of managing log

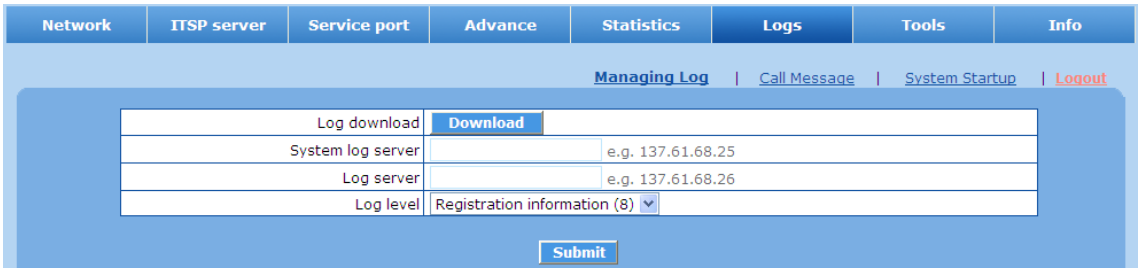


Table 2-11 Parameters of managing log

Name	Description
Log download	See the description below.
System log server	Set the IP address of system log server.
Log server	IP address of debugging log server
Log level	Select log level of the device, default value is 4. The setting range is 1-5, the higher the level goes, the more details the log file will be. Note: log level should be set to be 4 or lower when device is used in normal operation, avoiding influencing the system performance.

Procedure of downloading the debugging log:

Step1 Click **Download**, the device starts packing the log.

Step2 After few seconds, the interface of log saving will appear.

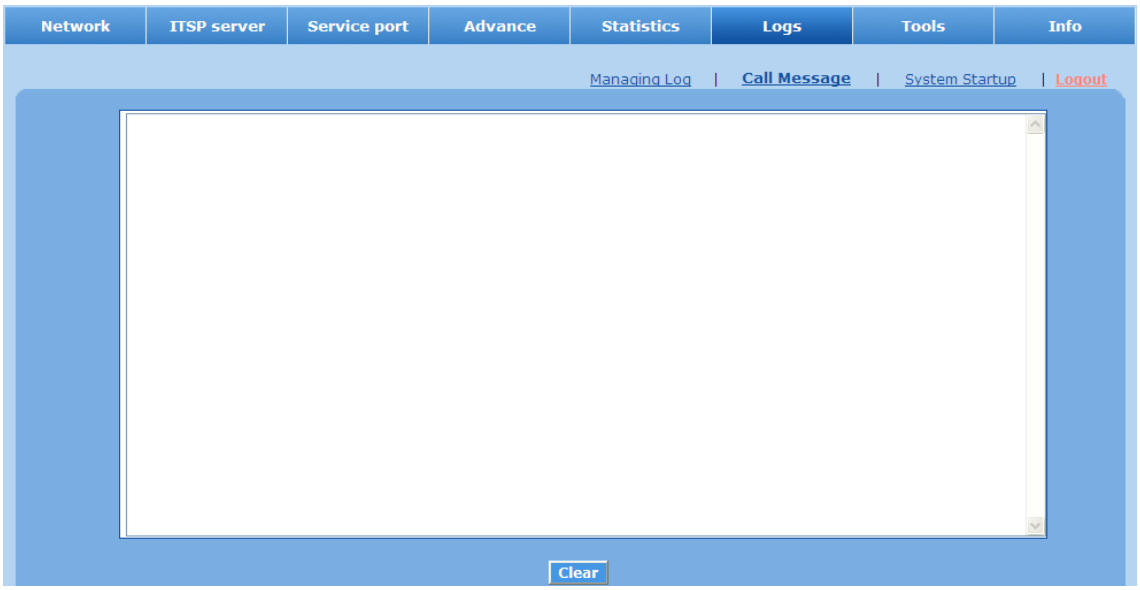
Step3 Click **Save**, and select the path to save.

Step4 The user may review the log from the server concerned.

2.8.2 Call Message

After login, click **Logs** > **Call Message**.

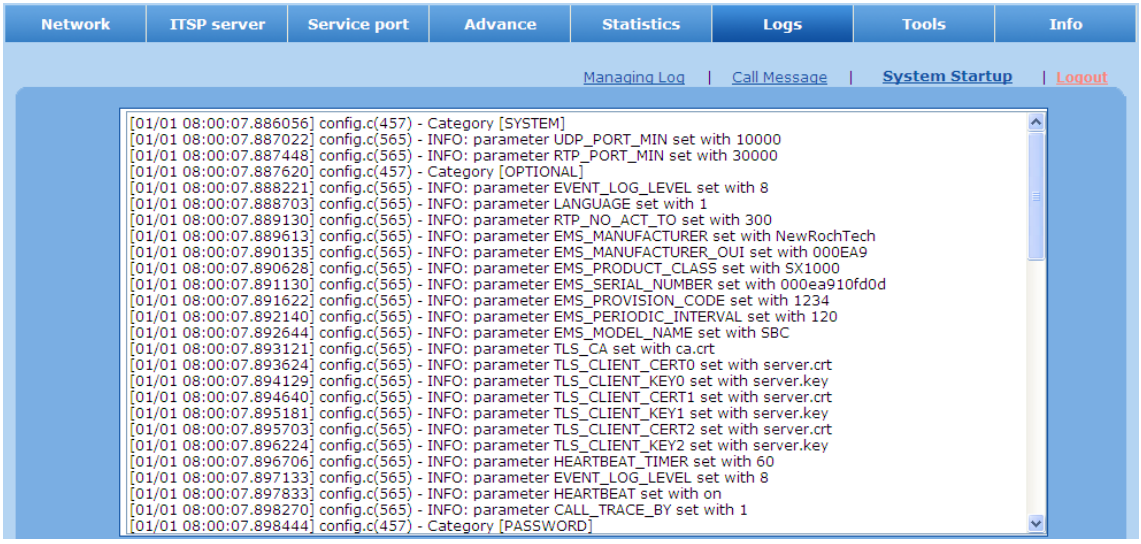
Figure 2-12 Call message interface



2.8.3 System Startup

After login, click **Logs** > **System startup**.

Figure 2-13 Interface of system startup



2.9 Tools

2.9.1 Change Password

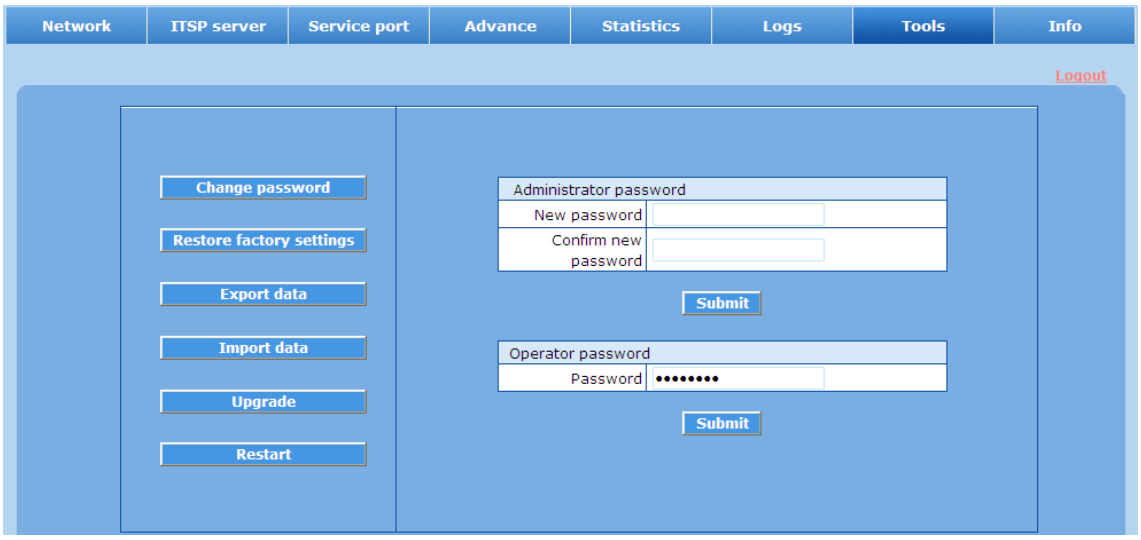
After login, click **Tools** to open this interface. Only administrator is entitled to change the password of

login.

For changing administrator password, it's required to enter new password into **New password** field and **Confirm new password** field, then click **Submit**.

The password being used by the operator will be displayed as hidden codes, which could be changed by the administrator at any time. The administrator is allowed to change the operator's password by entering the new password into **Operator password > password**.

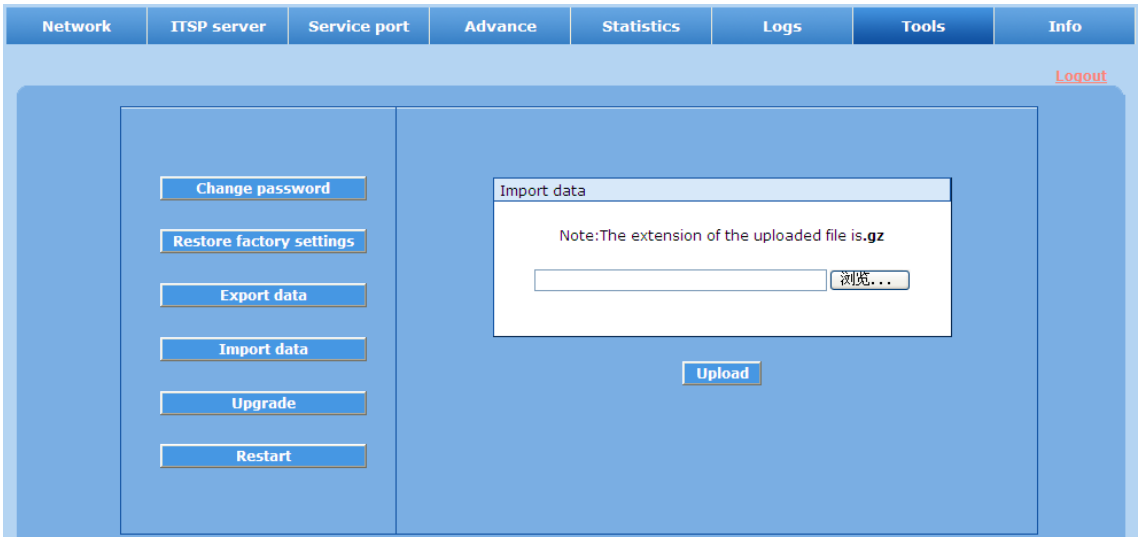
Figure 2-14 Interface of password changing



2.9.2 Import Data

After login, click **Tools>Import data** to open this interface. Operating procedure is the same as that of software upgrade.

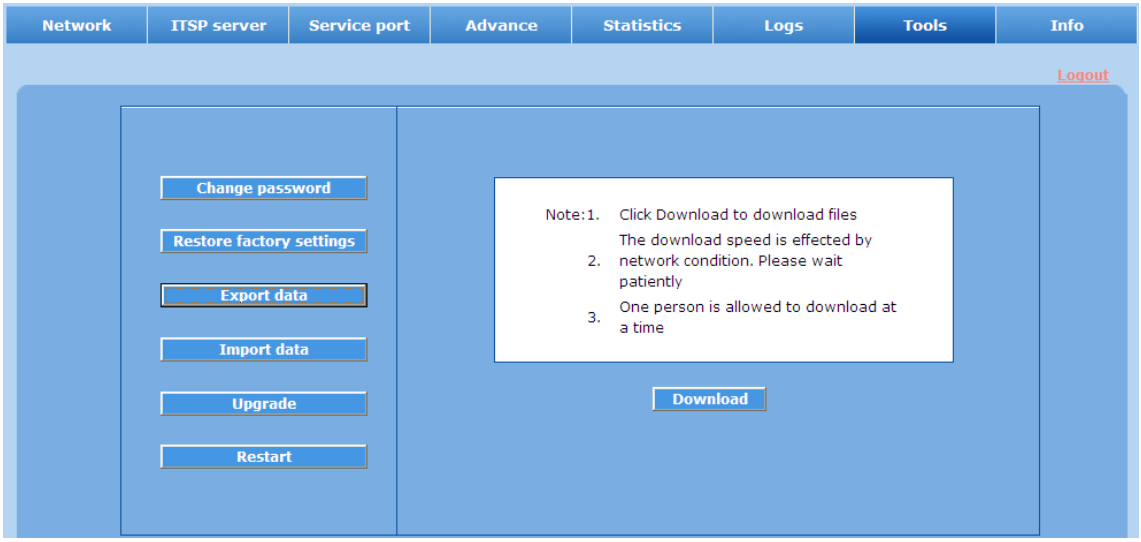
Figure 2-15 Interface of importing data



2.9.3 Export Data

After login, click **Tools** > **Export data** to open this interface. The download procedure is similar to the download procedure of log files.

Figure 2-16 Interface of exporting data



2.9.4 Upgrade

After login, click **Tools** > **Upgrade** to open this interface. The software upgrad procedure is presented as below:

Step1 Obtain the upgrade files (tar.gz file), and save the file onto a local computer.

Step2 Click **Tools** > **Upgrade** to access to the page of software upgrade.

Step3 Click **Browse** to select the upgrade files.

Step4 Click **Upload**.

Step5 Uploading will be completed in about 30 seconds, then click **Next**.

Step6 After success in upgrade, the following dialog will appear, click **Confirm**.

Note

- The software upgrade operation must be conducted on an 100M Ethernet port.
- A few minutes are needed to upgrade the device. Don't operate the device during this period.
- The device is on the progress of reboot when the interface cannot be displayed.
- Wait for about two minutes, and access the interface of device management system, click Version info and check the software version.

2.9.5 System Reboot

After login, click **Tools** > **Reboot** to restart the device. As this is a system wide reset, it takes longer time.

2.9.6 Restore Factory Settings

After login, click **Tools > Restore factory settings** to restore the factory settings.

The factory settings are designed based on common applications, and therefore, no need to modify them in many deployment situations.

2.10 Version Information

After login, click **Version info** to view the device hardware and software version information.

2.11 Logout

After login, click the **Logout** at top right to exit the device management system and return to the login interface.