Quick Configuration Guide

1.1 Scope of This Guide

This note is applicable to the SX1000 SBC product.

1.2 Introduction

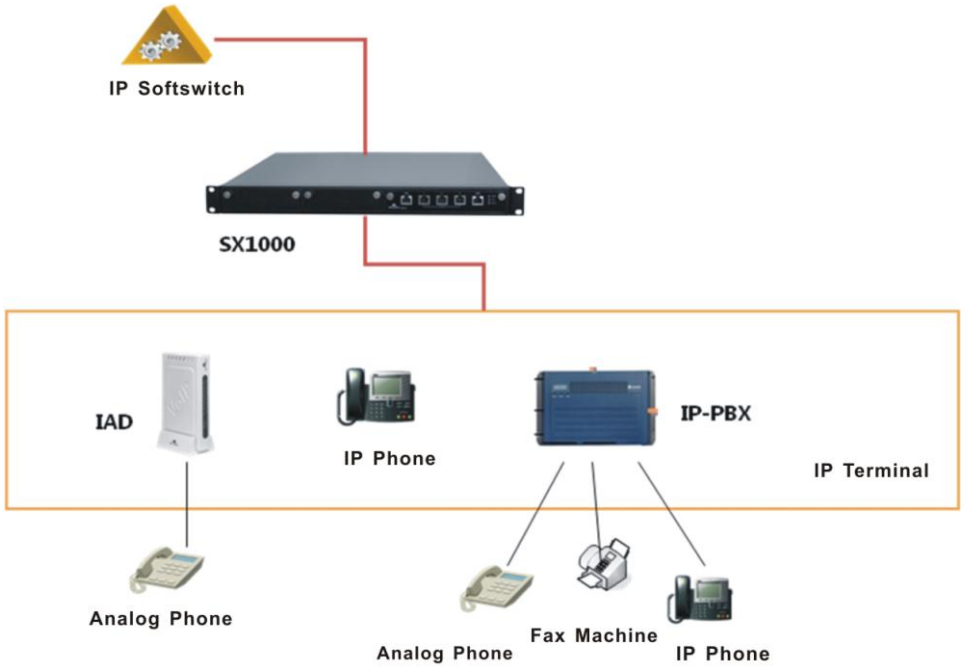
SX1000, an enterprise SBC (Session Border Controller), is a member of VoIP product family developed by New Rock Technologies, Inc. It interconnects voice communication over different IP networks and provides security schemes to protect the network from attacks and the privacy of communications. With highly compact design and the capacity of supporting 500 register users and 100 concurrent calls. SX1000 is a cost-effective enterprises solution to build voice VPN amount headquarter and branch offices.

This guide describes the basic functions and the configurations.

1.3 The Main Features and Advantages

- NAT/firewall traversal
- Registration and authentication of SIP terminal
- Encryption and decryption of signaling and voice media streams, including TLS/SRTP
- Access control through IP table
- RTP proxy
- Internetworking with up to three separate networks
- Surveillance and network failover
- Status and statistics report with TR069

The diagram below shows a typical deployment scenario of SX1000.



Note

The terminal devices, such as VoIP gateway, SIP phone, IP-PBX and soft-phone, are registered to the SIP registration server through SX1000. In this type of application, the terminal devices are not required to configure URL of the SIP registration server; instead, only the address of SX1000 and its designated service port are to be configured. Through the service port, the SX1000 receives the packets from the terminal devices and redirect them to the responding SIP softswitch with or without encryption.

1.4 Quick Configuration

1.4.1 Logon

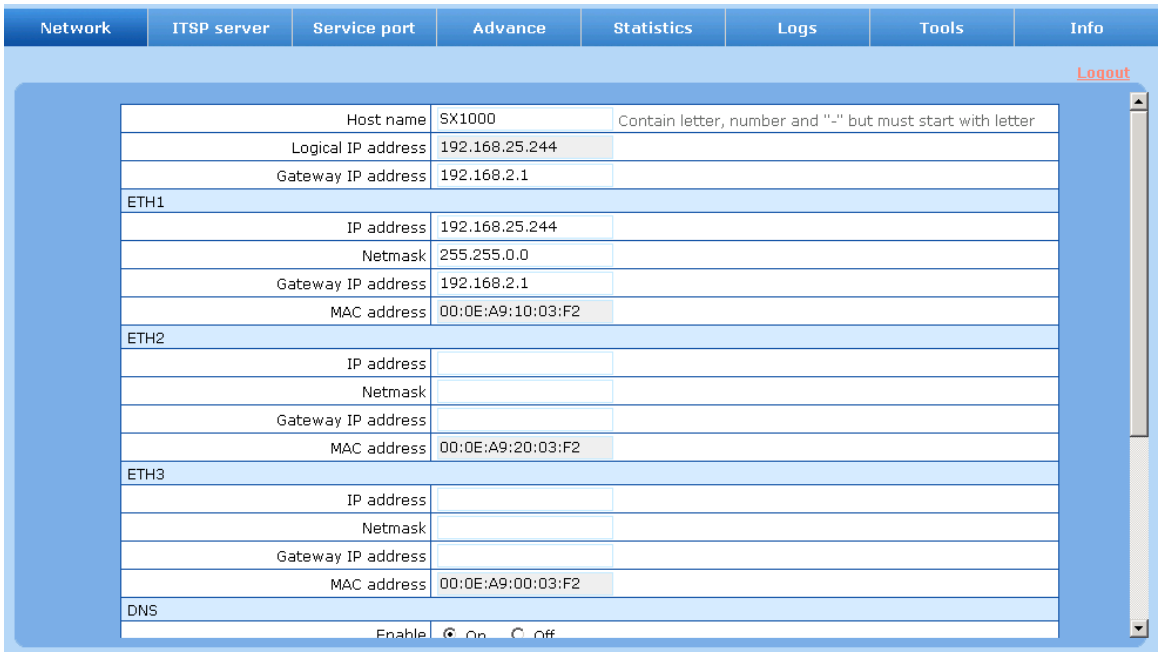
Enter the IP address of SX1000 in the address bar of the browser. Note that the factory default of ETH1 address is 192.168.2.240. Enter the password as either administrator or an operator, and the default password are sx1000 (lower case) and operator (lower case), respectively.

Note

It is recommended to use IE 7.0 or later version to perform the configurations.

1.4.2 Network Configuration

ETH1 is the factory default Ethernet port, and ETH2 or ETH3 can be enabled according to application. Fill in the network parameters, including IP address, netmask and gateway IP address fields, and click **Submit** to save the configuration.

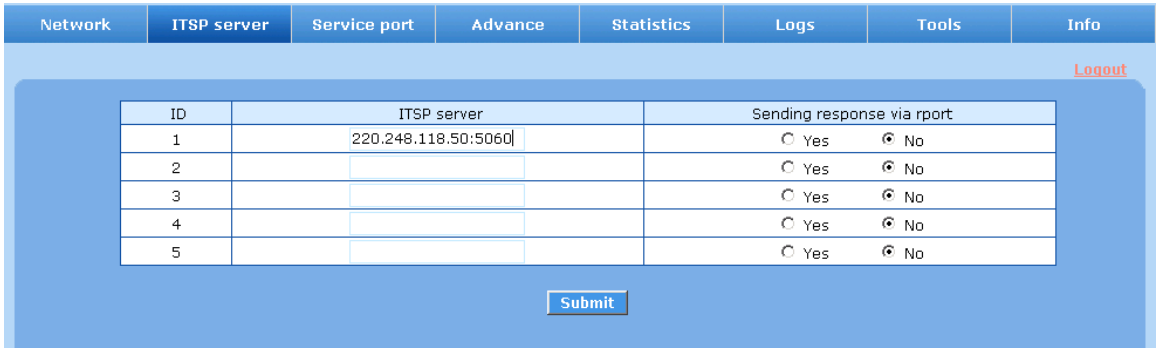


Note

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

1.4.3 ITSP Server Configuration

Click **ITSP** and enter the configuration interface of SIP proxy. Up to five 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, e.g. 200.248.118.50:5060. Select **Yes** for **Sending response to rport** if SX1000 needs to send response messages to the sending port of the proxy. Otherwise, select **No**.



Note

When SX1000 is deployed with Huawei SoftCo, it is recommended to use “No” for this parameter.

1.4.4 Service Port Configuration

Click **Service port** to configure the Ethernet ports.

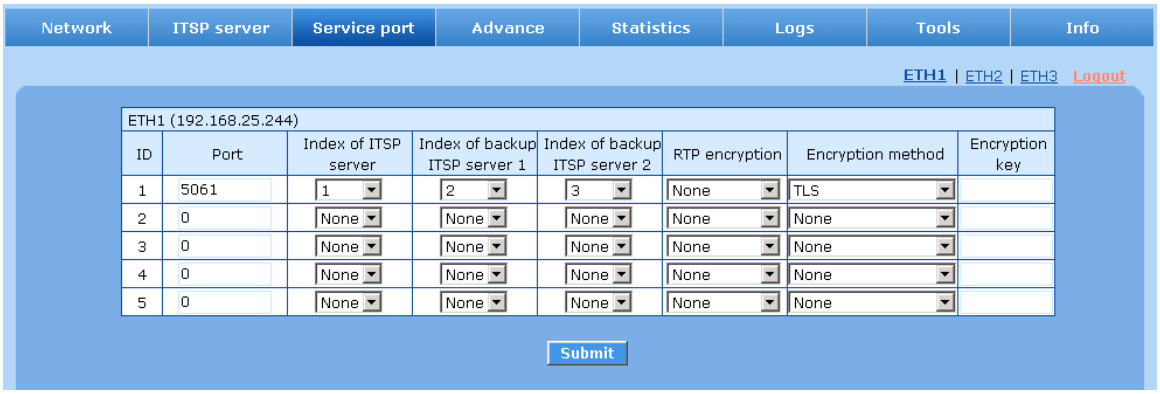
- The service port is used to receive the SIP messages from terminals, which will be processed and redirect to the ITSP softswitch associated to the port.
- Up to five service ports can be configured on SX1000, each associated with a primary softswitch and its backup softswitches.
- Up to two backup 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 it 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 three 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.

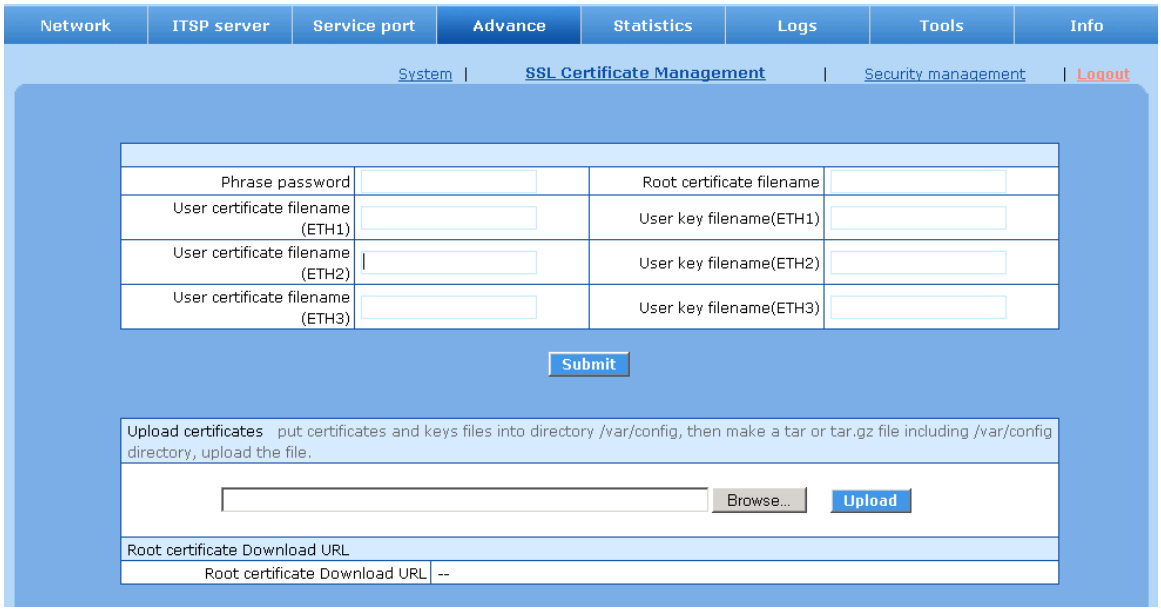


Note

When SX1000 is deployed with Huawei SoftCo, encryption schemes listed here are not recommended to use, other than TLS/SRTP towards the terminal side.

1.4.5 SSL Certificate Management

Click **Advance > SSL Certificate Management** to configure SSL certificate.



If TLS encryption is selected for service port, SSL certificate related parameters should be configured.

Upload the SSL certificate.

Refer to Section **Generating SSL certificate** for CA certificate making procedure.

Procedure I: Uploading the certificate from Web GUI of SX1000

- Create var/config under /tmp directory, and copy the root CA certificate, the custom CA certificate and the private key to var/config directory under Linux operation system;
- Compress the files together with the var/config directory in .tar or .tar.gz format to file ssl_cert.tar.gz;

- Upload file ssl_cert.tar.gz by ftp to the PC that administrator uses to logon to the SX1000;
- Login the Web GUI of SX1000, and enter SSL certification interface. Upload file ssl_cert.tar.gz to SX1000 and restart it.

Procedure II: Uploading the certificate from FTP server

- Copy the root CA certificate, the custom CA certificate and the private key to a FTP server;
- Telnet into SX1000 (username: root; password: voipgateway) and type cd/var/config to enter config directory;
- Enter ftp xxx.xxx.xxx.xxx (IP address of ftp server). Then enter username and password of FTP server to login to it;
- Enter get ca.crt to download the root CA certificate to SX1000;
- Enter get client.crt to download the custom CA certificate to SX1000;
- Enter get client.key to download the custom CA certificate to SX1000;
- Enter bye to logout of ftp server
- Enter reboot to restart SX1000.

The description of 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 (ETH n)	The name of the file which contains the custom CA certificate for ETH n.
User key filename (ETH n)	The name of the file which contains the custom private key for ETH n.

When there is only one Ethernet port which is configured with TLS encryption, there is no need to setup the custom CA certificate and the private key to other Ethernet ports.

1.4.6 Security Management

Click **Advance > Security** to configure security related parameters.

Telnet service can be disabled or enabled on the **Advanced > 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.

1.4.7 Generating SSL Certificate

Create root CA

Step1 Create RSA private key for the root CA (it is suggested to set the length of key as 512 bits)

openssl genrsa -des3 -out ca.key 512

You should enter a stream of characters, when you will be prompted to enter the password, and this password should be used throughout the procedure.

The private key will be generated in ca.key.

Step2 Create a self-signed CA certificate with the private key generated in the above steps, using the following command:

openssl req -new -x509 -days 9000 -key ca.key -out ca.crt

Enter the password when you are prompted for the password. You need to enter related information when you are prompted as in the following example:

Country<97> CA, for example

State or Province<97>British Columbia

Locality (city or town)<97>Burnaby

Organization Name<97>NerockTech Inc

Organizational Unit Name<97>Voice

Common Name<97>NewrockCA

E-mail address<97>admin@newrocktech.com

The CA certificate file is generated.

Creating the custom CA certificate

Step1 Create a RSA private key (it is suggested to set the length of the key as 512 bits) using the following command:

openssl genrsa -out client.key 512

Enter the password when you are prompted.

The private key file client.key is generated.

Step2 Create custom certificate signing request (CRS) using the following command:

openssl req -new -key client.key -out client.csr

Enter the related information when you are prompted as in the following example:

Country<97> CA, for example

State or Province<97>British Columbia

Locality (city or town)<97>Burnaby

Organization Name<97>NewrockTech Inc

Organizational Unit Name<97>Voice

Common Name<97>the IP address of the Ethernet port of SX1000

E-mail address<97>admin@newrocktech.com

Enter the password when you are prompted for the password.

An optional company name: NewRock

The file client.csr is generated.

Step3 Create custom CA certificate signed by this CA certificate using the following command:

openssl x509 -days 9000 -CA ca.crt -CAkey ca.key -req -CAcreateserial -CAserial ca.srl -in client.csr -out client.crt

Enter the password when you are prompted for the password.

The custom CA certificate file client.crt is generated.

Note

In the Common Name command in the example above, the IP address of the Ethernet port on SX1000 should be entered. For example, when TLS is used for ETH1, the IP address of ETH1 should be filled in generating CA certificate. Further, on the SSL management interface of SX1000, the client.crt and the client.key should be filled in User certificate filename (ETH1) and User key filename (ETH1) fields, respectively.

1.5 Special Note

When SX1000 is deployed with Huawei SoftCo, it is recommended to use the factory default of the following parameters.

Web GUI	Parameters	Factory default
ITSP server	Sending response via port	No
Service port	RTP encryption	None
Advance	RTP proxy	yes
Advance	RTP disconnect timeout	300
Advance	NAT traversal	On