SRTP&TLS

Secure Real-Time Transport Protocol

Secure Real-Time Transport Protocol (SRTP) provides means of encrypting the RTP streams during VoIP phone calls to avoid interception and eavesdropping. The parties participating in the call should enable the SRTP feature simultaneously. When this feature is enabled on both phones, the IP phone will negotiate with the other phone what type of encryption to utilize for the session. This negotiation process is compliant with RFC 4568.

When a user places a call on the enabled SRTP phone, the IP phone sends an INVITE message with the RTP encryption algorithm to the destination phone.

The sample of the RTP encryption algorithm carried in the SDP of the INVITE message for reference:

```
m=audio 11780 RTP/SAVP 0 8 18 9 101
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:NzFlNTUwZDk2OGVlOTc3YzNkYTkwZWVkMTM1YWFj
a=crypto:2 AES_CM_128_HMAC_SHA1_32
inline:NzkyM2FjNzQ2ZDgxYjg0MzQwMGVmMGUxMzdmNWFm
a=crypto:3 F8_128_HMAC_SHA1_80 inline:NDliMWIzZGE1ZTAwZjA5ZGFhNjQ5YmEANTMzYzA0
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:9 G722/8000
a=fmtp:101 0-15
a=rtpmap:101 telephone-event/8000
a=ptime:20
a=sendrecv
```

The callee receives the INVITE message with the RTP encryption algorithm. The callee answers the call and responses with a 200 OK message carrying the negotiated RTP encryption algorithm.

The sample of the RTP encryption algorithm carried in the SDP of the 200 OK message for reference:

```
m=audio 11780 RTP/SAVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:NGY4OGViMDYzZjQzYTNiOTNkOWRiYzRlMjM0Yzcz
a=sendrecv
a=ptime:20
a=fmtp:101 0-15
```

You can configure the SRTP feature on a per-account basis. When SRTP is enabled on both phones, the RTP streams will be encrypted, and a lock icon appears on the LCD screen of each IP phone after the successful negotiation.

Note If you enable SRTP, then you should also enable TLS. This ensures the security of SRTP encryption. For more information on TLS, refer to

Procedure

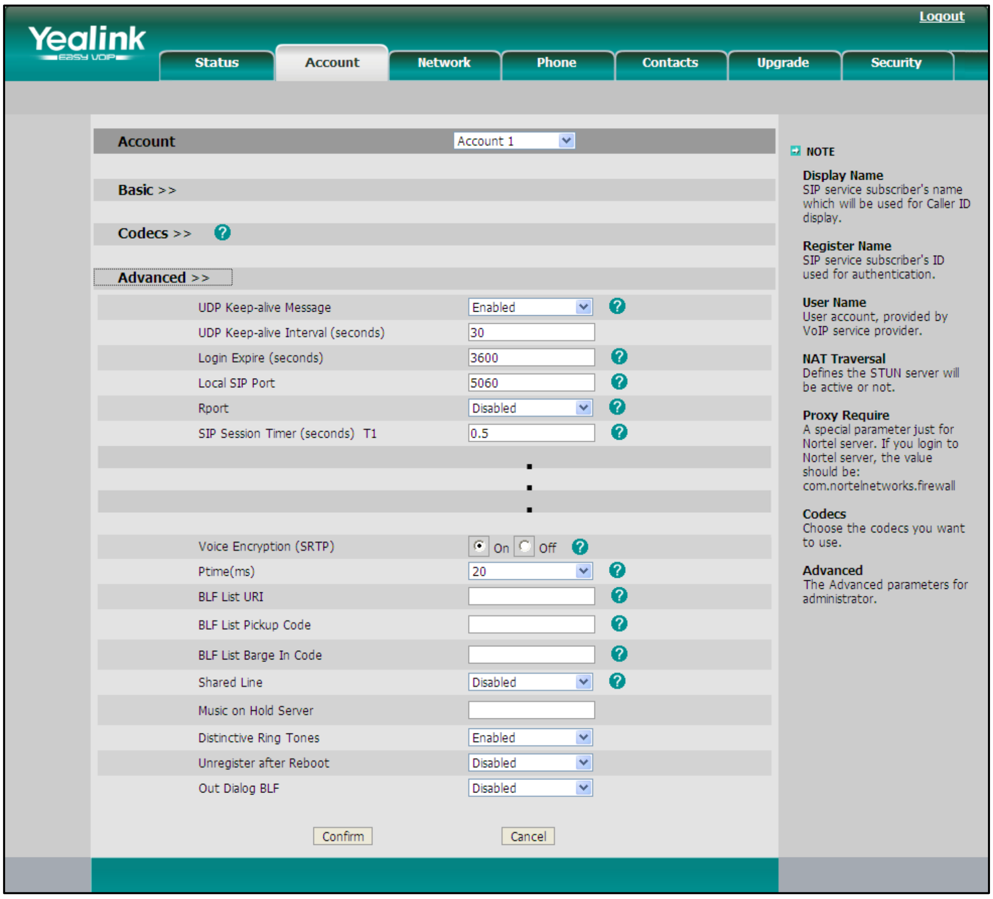
SRTP can be configured using the configuration files or locally.

Configuration File	<MAC>.cfg	Configure the SRTP feature on a per-account basis. For more information, refer to **错误!未找到引用源。** on page 错误!未定义书签。.
Local	Web User Interface	Configure the SRTP feature on a per-account basis. **Navigate to**: http://<phoneIPAddress>/cgi-bin/ConfigManApp.com?Id=4

To configure the SRTP feature via web user interface:

1. Click on **Account**.
2. Select the desired account from the pull-down list of **Account**.
3. Click on **Advanced>>**.

4. Mark the desired radio box in the **Voice Encryption (SRTP)** field.



Account: Account 1

Basic >>

Codecs >>

Advanced >>

UDP Keep-alive Message	Enabled
UDP Keep-alive Interval (seconds)	30
Login Expire (seconds)	3600
Local SIP Port	5060
Rport	Disabled
SIP Session Timer (seconds) T1	0.5
Voice Encryption (SRTP)	● On ○ Off
Ptime(ms)	20
BLF List URI	
BLF List Pickup Code	
BLF List Barge In Code	
Shared Line	Disabled
Music on Hold Server	
Distinctive Ring Tones	Enabled
Unregister after Reboot	Disabled
Out Dialog BLF	Disabled

NOTE

Display Name
SIP service subscriber's name which will be used for Caller ID display.

Register Name
SIP service subscriber's ID used for authentication.

User Name
User account, provided by VoIP service provider.

NAT Traversal
Defines the STUN server will be active or not.

Proxy Require
A special parameter just for Nortel server. If you login to Nortel server, the value should be: com.nortelnetworks.firewall

Codecs
Choose the codecs you want to use.

Advanced
The Advanced parameters for administrator.

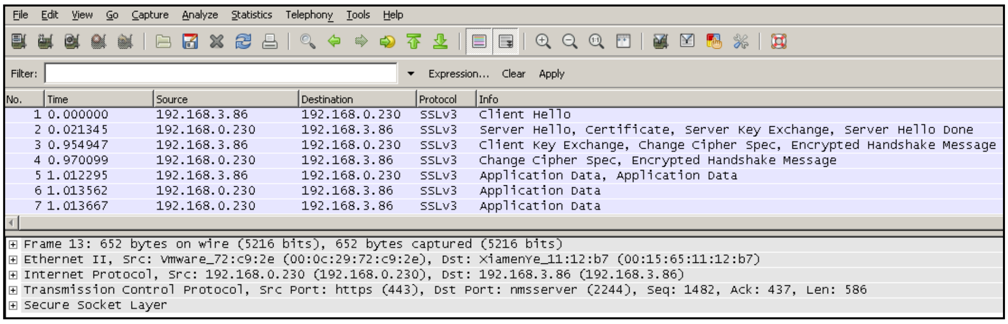
5. Click **Confirm** to accept the change.

Transport Layer Security

The TLS protocol is a commonly-used protocol for providing communications privacy and managing the security of message transmission. The TLS allows the IP phone to communicate with other remote parties and connect to the HTTPS URL for provisioning in a way that is designed to prevent eavesdropping and tampering.

The TLS protocol is composed of two layers: the TLS Record Protocol and the TLS Handshake Protocol. The TLS Record Protocol completes the actual data transmission and ensures the integrity and privacy of the data. The TLS Handshake Protocol allows the server and client to authenticate each other and negotiate an encryption algorithm and cryptographic keys before data is exchanged.

The following figure illustrates the TLS messages exchanged between the IP phone and TLS server to establish an encrypted communication channel:


File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

```
No.  Time      Source         Destination    Protocol  Info
  1 0.000000   192.168.3.86   192.168.0.230  SSLv3     Client Hello
  2 0.021345   192.168.0.230  192.168.3.86   SSLv3     Server Hello, Certificate, Server Key Exchange, Server Hello Done
  3 0.954947   192.168.3.86   192.168.0.230  SSLv3     Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  4 0.970099   192.168.0.230  192.168.3.86   SSLv3     Change Cipher Spec, Encrypted Handshake Message
  5 1.012295   192.168.3.86   192.168.0.230  SSLv3     Application Data, Application Data
  6 1.013562   192.168.0.230  192.168.3.86   SSLv3     Application Data
  7 1.013667   192.168.0.230  192.168.3.86   SSLv3     Application Data

⊞ Frame 13: 652 bytes on wire (5216 bits), 652 bytes captured (5216 bits)
⊞ Ethernet II, Src: Vmware_72:c9:2e (00:0c:29:72:c9:2e), Dst: XiamenYe_11:12:b7 (00:15:65:11:12:b7)
⊞ Internet Protocol, Src: 192.168.0.230 (192.168.0.230), Dst: 192.168.3.86 (192.168.3.86)
⊞ Transmission Control Protocol, Src Port: https (443), Dst Port: nmsserver (2244), Seq: 1482, Ack: 437, Len: 586
⊞ Secure Socket Layer
```

Step1: IP phone sends "Client Hello" message proposing SSL options.

Step2: Server responds with "Server Hello" message selecting the SSL options, sends its public key information in "Server Key Exchange" message and concludes its part of the negotiation with "Server Hello Done" message.

Step3: IP phone sends session key information (encrypted with server's public key) in the "Client Key Exchange" message.

Step4: Server sends "Change Cipher Spec" message to activate the negotiated options for all future messages it will send.

The IP phone can encrypt SIP with TLS, which is called SIPS. When TLS is enabled for an account, the SIP message of this account will be encrypted, and a lock icon appears on the phone LCD screen after the successful TLS negotiation. You can specify the IP phone to encrypt the SIP signal using the RC4 encryption algorithm.

In order to use the TLS on the IP phone, you need to perform the following steps:

- Uploading certificates to the IP phone
- Configuring the IP phone to use the TLS

Certificates

The IP phone can serve as a TLS client or a TLS server. The TLS requires the following security certificates to perform the TLS handshake:

- **Trusted Certificate**: When the IP phone requests a TLS connection with a server, the IP phone should verify the certificate sent by the server to decide whether the server is trusted based on the trusted certificates list. You can upload up to 10 trusted certificates to the IP phone.
- **Server Certificate**: When the other clients request a TLS connection with the IP phone, the IP phone sends the server certificate to the clients for authentication. You can only upload one server certificate to the IP phone. The old server certificate will be overwritten by the new one.

You can configure the "Only Accepted Trusted Certificates" feature on the IP phone. If enabled, the IP phone will check the certificate sent by the server and only accept the certificates listed in the Trusted Certificates list. You can configure the TLS on a per-account basis.

Procedure

Configuration changes can be performed using the configuration files or locally.

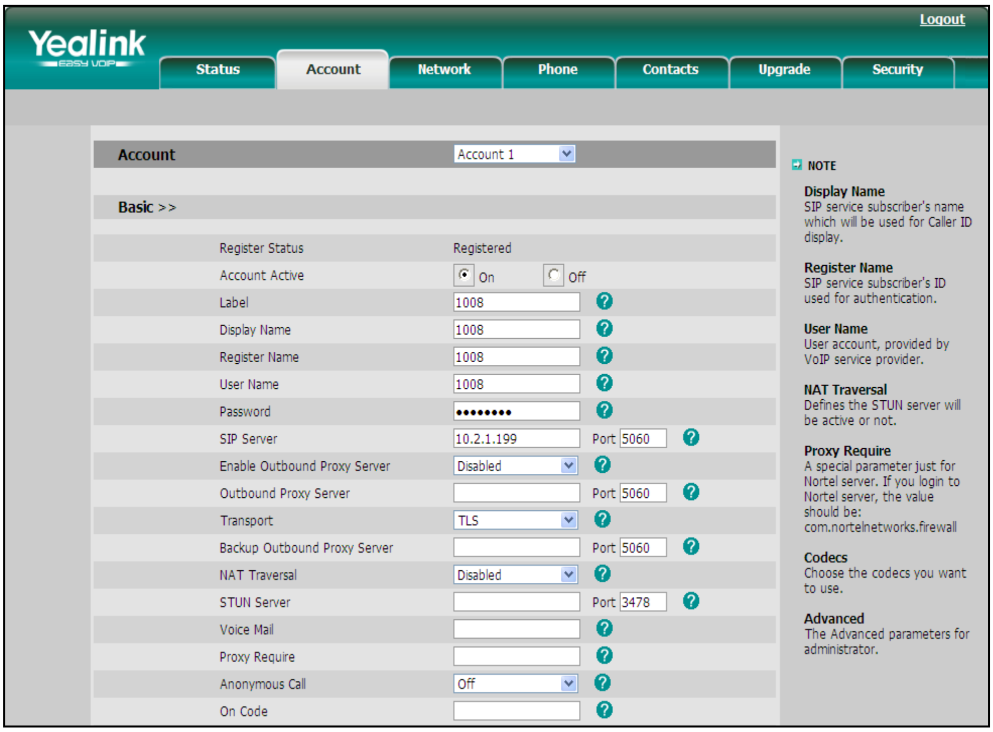
Configuration File	<MAC>.cfg	Configure the IP phone to use TLS and authenticate the connected server. For more information, refer to 错误!未找到引用源。 on page 错误!未定义书签。. Specify the IP phone to encrypt the SIP signal using RC4 encryption algorithm. For more information, refer to 错误!未找到引用源。 on page 错误!未定义书签。.
	<y0000000000xx>.cfg	Upload certificates to the IP phone. For more information, refer to 错误!未找到引用源。 on page 错误!未定义书签。.
Local	Web User Interface	Configure the IP phone to use TLS. **Navigate to**: http://<phoneIPAddress>/cgi-bin/ConfigManApp.com?Id=4 Specify the IP phone to encrypt the SIP signal using RC4 encryption algorithm. **Navigate to**: http://<phoneIPAddress>/cgi-bin/ConfigManApp.com?Id=4 Upload the certificates to the IP phone. **Navigate to**: http://<phoneIPAddress>/cgi-bin/ConfigManApp.com?Id=32 Configure the IP phone to authenticate the connected server. **Navigate to**: http://<phoneIPAddress>/cgi-b

		in/ConfigManApp.com?Id=33

To configure TLS via web user interface:

1. Click on **Account**.
2. Select the desired account from the pull-down list of **Account**.

3. Select **TLS** from the pull-down list of the **Transport**.



Account Account 1

Basic >>

Register Status	Registered
Account Active	● On ○ Off
Label	1008
Display Name	1008
Register Name	1008
User Name	1008
Password	••••••••
SIP Server	10.2.1.199 Port 5060
Enable Outbound Proxy Server	Disabled
Outbound Proxy Server	Port 5060
Transport	TLS
Backup Outbound Proxy Server	Port 5060
NAT Traversal	Disabled
STUN Server	Port 3478
Voice Mail	
Proxy Require	
Anonymous Call	Off
On Code	

NOTE

Display Name
SIP service subscriber's name which will be used for Caller ID display.

Register Name
SIP service subscriber's ID used for authentication.

User Name
User account, provided by VoIP service provider.

NAT Traversal
Defines the STUN server will be active or not.

Proxy Require
A special parameter just for Nortel server. If you login to Nortel server, the value should be: com.nortelnetworks.firewall

Codecs
Choose the codecs you want to use.

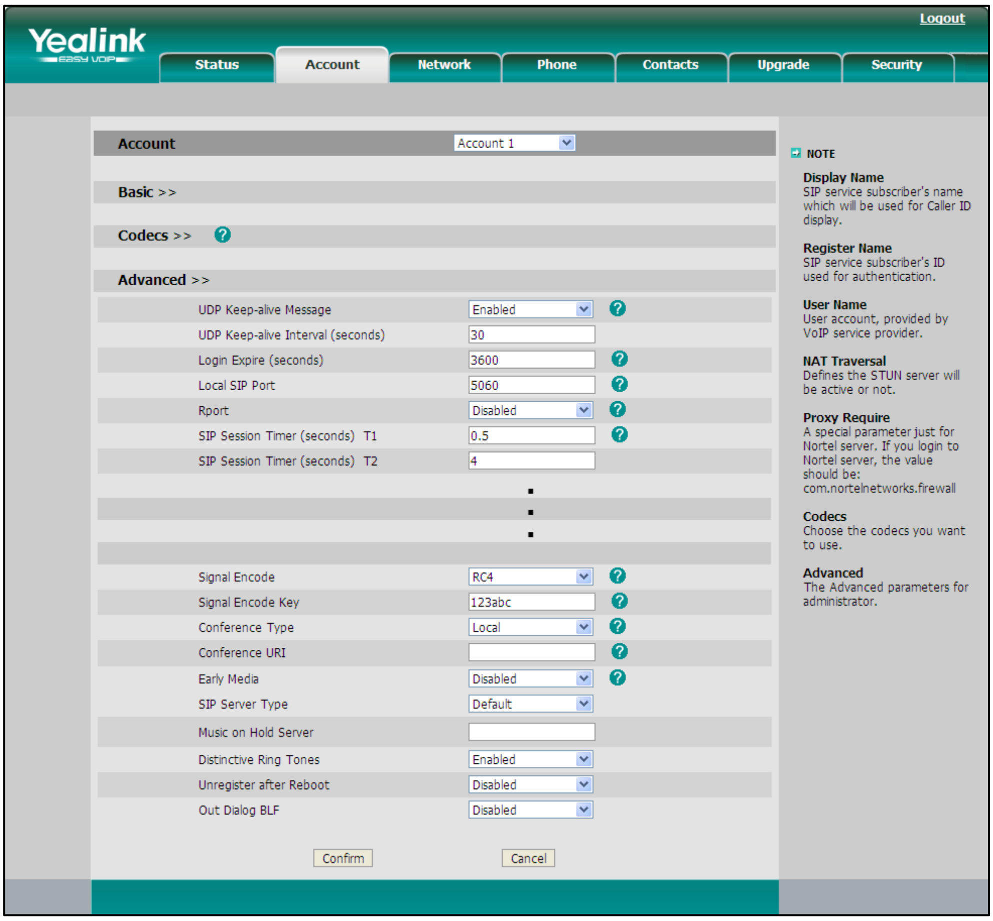
Advanced
The Advanced parameters for administrator.

4. Click **Confirm** to accept the change.

To Specify the IP phone to encrypt the SIP signal using RC4 encryption algorithm:

1. Click on **Account**.
2. Select the desired account from the pull-down list of **Account**.
3. Click on **Advanced>>**.

4. Select **RC4** from the pull-down list of **Signal Encode**.



Account: Account 1

Basic >>

Codecs >>

Advanced >>

UDP Keep-alive Message: Enabled

UDP Keep-alive Interval (seconds): 30

Login Expire (seconds): 3600

Local SIP Port: 5060

Rport: Disabled

SIP Session Timer (seconds) T1: 0.5

SIP Session Timer (seconds) T2: 4

Signal Encode: RC4

Signal Encode Key: 123abc

Conference Type: Local

Conference URI:

Early Media: Disabled

SIP Server Type: Default

Music on Hold Server:

Distinctive Ring Tones: Enabled

Unregister after Reboot: Disabled

Out Dialog BLF: Disabled

NOTE

Display Name
SIP service subscriber's name which will be used for Caller ID display.

Register Name
SIP service subscriber's ID used for authentication.

User Name
User account, provided by VoIP service provider.

NAT Traversal
Defines the STUN server will be active or not.

Proxy Require
A special parameter just for Nortel server. If you login to Nortel server, the value should be: com.nortelnetworks.firewall

Codecs
Choose the codecs you want to use.

Advanced
The Advanced parameters for administrator.

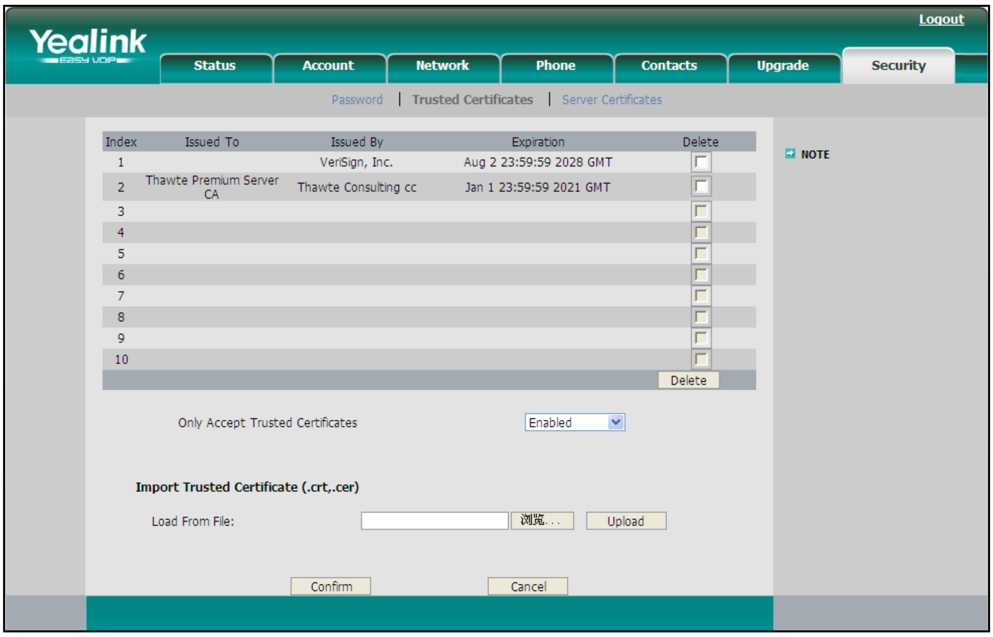
5. Enter the desired key in the **Signal Encode Key** field.

6. Click **Confirm** to accept the change.

To configure Only Accepted Trusted Certificates via web user interface:

1. Click on **Security**->**Trusted Certificates**.

2. Select the desired value from the pull-down list of **Only Accept Trusted Certificates**.



Index	Issued To	Issued By	Expiration	Delete
1		VeriSign, Inc.	Aug 2 23:59:59 2028 GMT	□
2	Thawte Premium Server CA	Thawte Consulting cc	Jan 1 23:59:59 2021 GMT	□
3				□
4				□
5				□
6				□
7				□
8				□
9				□
10				□

Only Accept Trusted Certificates: Enabled

Import Trusted Certificate (.crt,.cer)

Load From File:

3. Click **Confirm** to accept the change.

To upload the trusted certificate via web user interface:

1. Click on **Security**->**Trusted Certificates**.

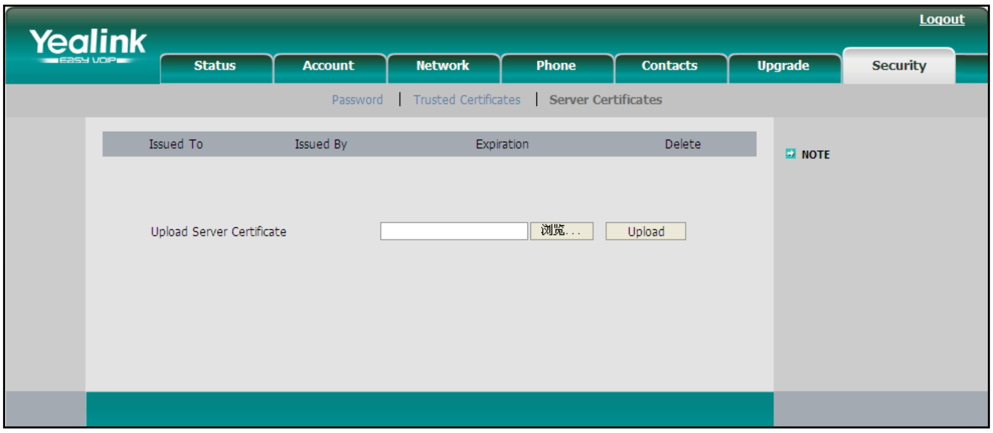
2. Click **Browse** to select the trusted certificate (*.crt or *.cer) from your local system.

3. Click **Upload** to upload the trusted certificate.

To upload the server certificate via web user interface:

1. Click on **Security**->**Server Certificates**.

2. Click **Browse** to select the server certificate (*.pem) from your local system.



Issued To	Issued By	Expiration	Delete

Upload Server Certificate

3. Click **Upload** to upload the server certificate.

The web user interface pops up the dialog box to prompt "Success: The Server

Certificate has been loaded! Rebooting, please wait…”.