

راه اندازی TLS/SRTP در تلفن های Akuvox و مرکز تلفن Yeastar

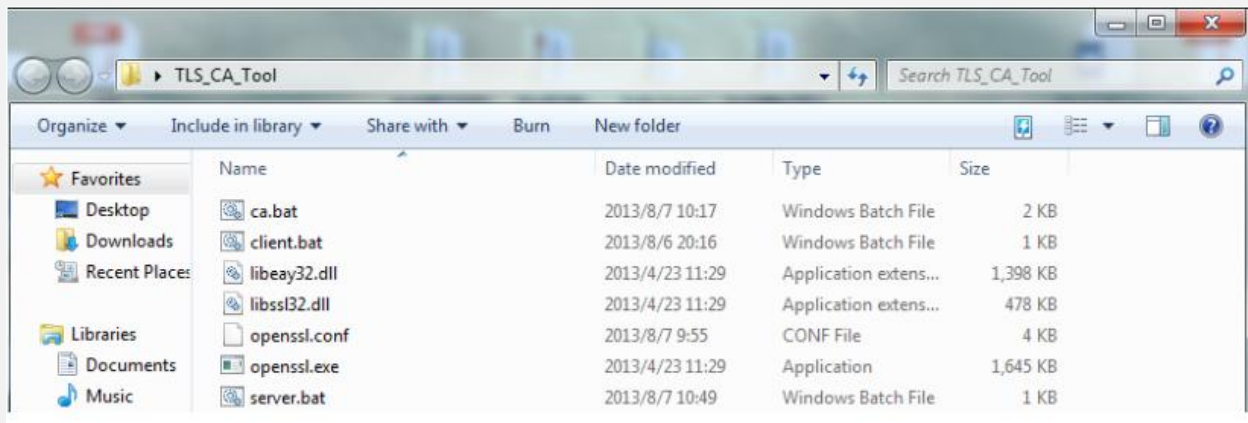
یکی از قابلیت‌هایی که تلفن‌های تحت شبکه آکووکس پشتیبانی می‌کنند قابلیت استفاده از TLS به جای UDP برای سیگنالینگ و همچنین SRTP برای امنیت انتقال صدا می‌باشد.

در این آموزش ما از یک تلفن مدل **Akuvox R59P** به عنوان کلاینت و از مرکز تلفن **Yeastar** استفاده خواهیم کرد.
***نکته بسیار مهم:** لازم به ذکر است در صورت صحیح نبودن تنظیمات تاریخ و ساعت بر روی تلفن، ارتباط TLS در نهایت برقرار نخواهد شد. بنابراین بهتر است قبل از شروع تنظیمات، تاریخ و ساعت تلفن را بررسی و در صورت اشتباه بودن آن را اصلاح کنید.

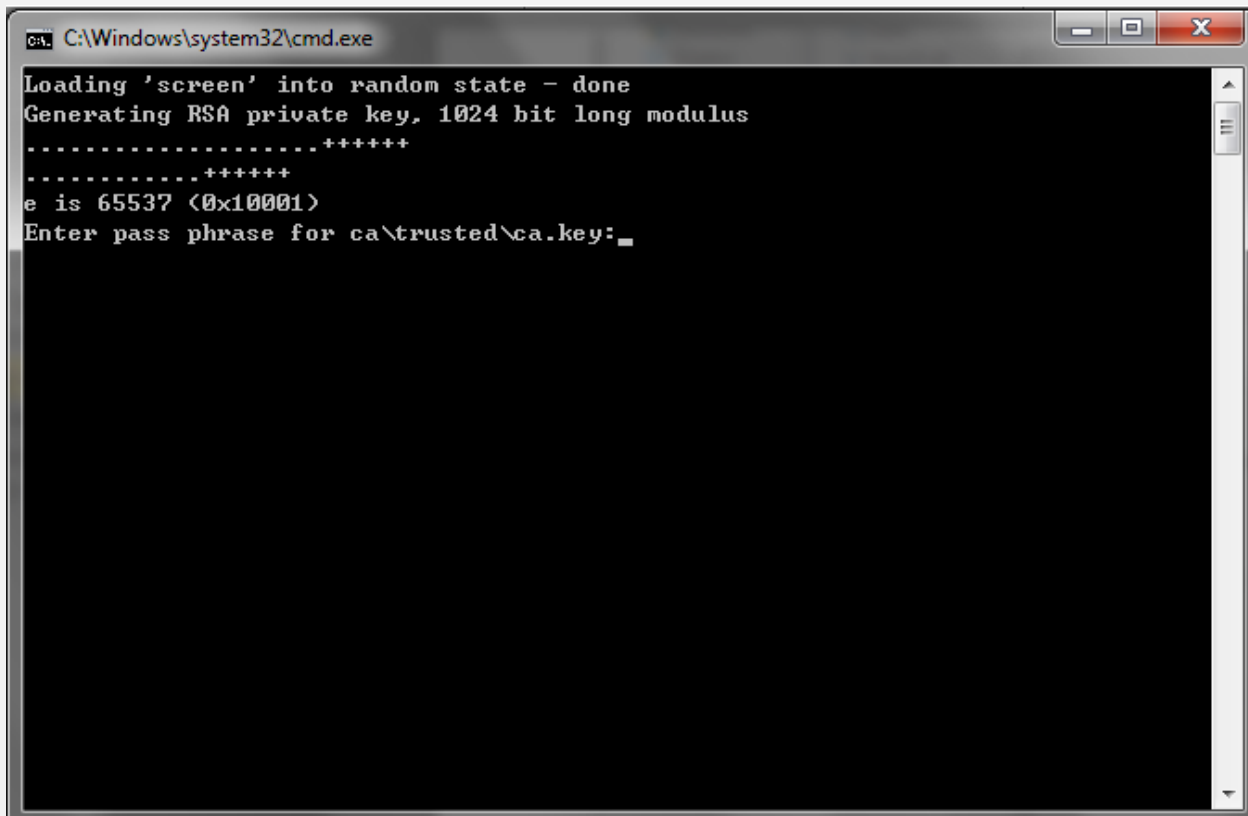
تنظیمات:

گام اول: ساخت Certificate

در ابتدا لازم است تا یک certificate برای مرکز تلفن **Yeastar** ایجاد نمایید. برای این کار ابتدا فایل **TLS CA Tool** را دانلود کرده و از حالت فشرده خارج کنید.



در مرحله‌ی اول روی **ca.bat** کلیک کرده و در صفحه اول ابتدا یک رمز دلخواه برای **ca key** وارد نمایید.



نکته: برای پارامتر common name آدرس آی پی سرور Yeastar را وارد کنید.

```

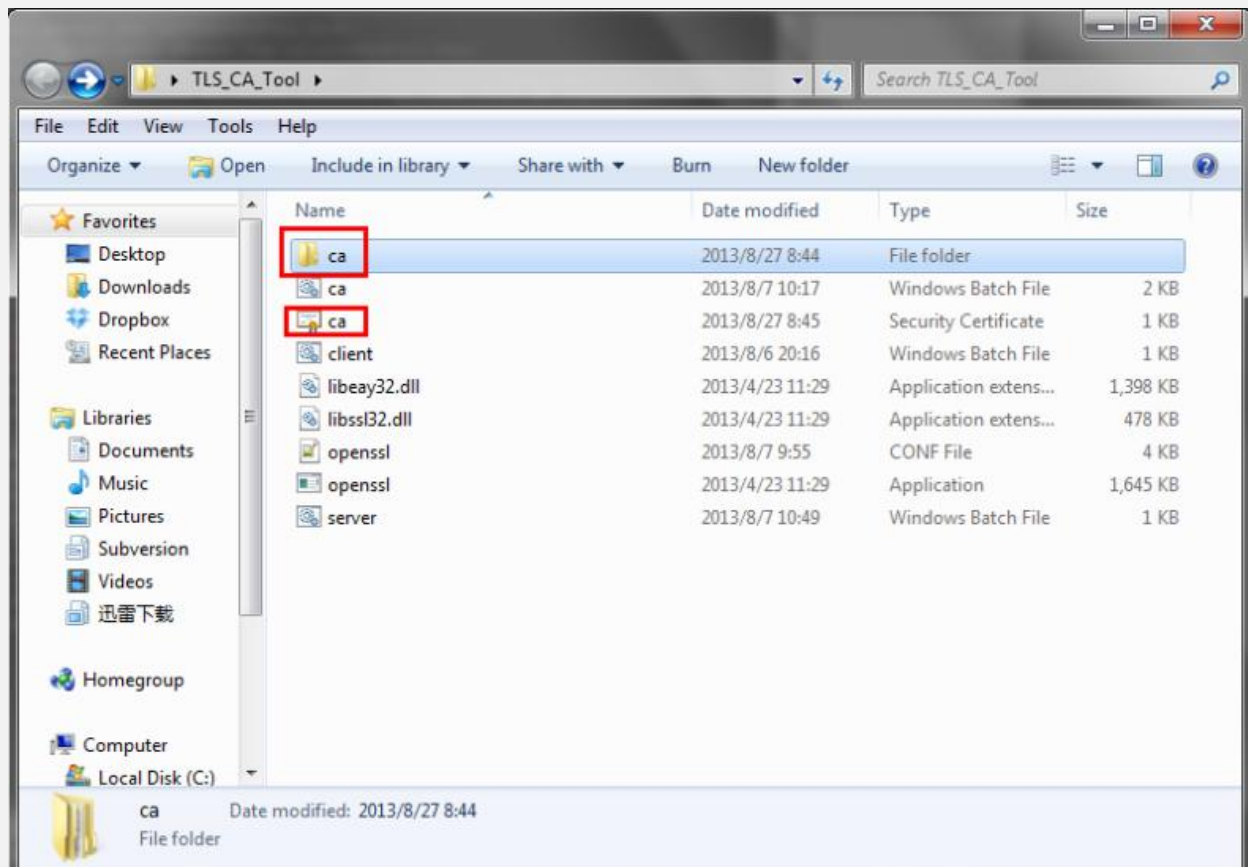
C:\Windows\system32\cmd.exe

What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

-----
Country Name <2 letter code> [CN]:CN
State or Province Name <full name> [Some-State]:FJ
Locality Name <eg, city> [L]:XM
Organization Name <eg, company> [Internet Widgits Pty Ltd]:Yeastar
Organizational Unit Name <eg, section> [O]:
Common Name< eg, ip address, website> [C]:192.168.6.216
Common Name1 <eg, ip address, website> [C]:
Common Name2 <eg, ip address, website> [C]:
Email Address [E]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password [challenge]:ys123456
An optional company name [company]:
Loading 'screen' into random state - done
Signature ok
subject=/C=CN/ST=FJ/L=XM/O=Yeastar/CN=192.168.6.216
Getting Private key
Enter pass phrase for ca\trusted\ca.key:
Press any key to continue . . .
    
```

در حال حاضر در پوشه فعلی یک فایل ca و یک فولدر ca ساخته شده است، لازم به ذکر است فایل ca که داخل پوشه ca قرار دارد با فایل ca در همین پوشه یکی می باشد.



در مرحله دوم روی فایل `server.bat` کلیک کرده و اطلاعات را دقیقاً مانند `ca.bat` که در مرحله قبل وارد شد وارد نمایید. در نهایت برای سوال اول و دوم "y" وارد کرده و Enter کنید.

```

C:\Windows\system32\cmd.exe
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:CN
State or Province Name (full name) [Some-State]:FJ
Locality Name (eg, city) []:XM
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Yeastar
Organizational Unit Name (eg, section) []:
Common Name0 (eg, ip address, website) []:192.168.6.216
Common Name1 (eg, ip address, website) []:
Common Name2 (eg, ip address, website) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:ys123456
An optional company name []:
Using configuration from openssl.conf
Loading 'screen' into random state - done
Enter pass phrase for ca\trusted\ca.key:
15140:error:28069065:lib(40):UI_set_result:result too small:./crypto/ui/ui_lib.c
:847:You must type in 4 to 511 characters
Enter pass phrase for ca\trusted\ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName          :PRINTABLE:'CN'
stateOrProvinceName  :PRINTABLE:'FJ'
localityName         :PRINTABLE:'XM'
organizationName     :PRINTABLE:'Yeastar'
commonName           :PRINTABLE:'192.168.6.216'
Certificate is to be certified until Mar  1 11:41:22 2027 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]:y
  
```

در نهایت فایل `asterisk.pem` داخل فولدر فعلی ساخته خواهد شد
 حال برای مرحله سوم روی `client.bat` کلیک کرده و مجدد مانند مراحل قبل اطلاعات را وارد کنید.

```

C:\Windows\system32\cmd.exe
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [CN]:CN
State or Province Name (full name) [Some-State]:FJ
Locality Name (eg, city) []:XM
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Yeastar
Organizational Unit Name (eg, section) []:
Common Name0 (eg, ip address, website) []:192.168.6.113
Common Name1 (eg, ip address, website) []:
Common Name2 (eg, ip address, website) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:ys123456
An optional company name []:
Using configuration from openssl.conf
Loading 'screen' into random state - done
Enter pass phrase for ca\trusted\ca.key:
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName       :PRINTABLE:'CN'
stateOrProvinceName :PRINTABLE:'FJ'
localityName      :PRINTABLE:'XM'
organizationName  :PRINTABLE:'Yeastar'
commonName        :PRINTABLE:'192.168.6.113'
Certificate is to be certified until Mar  1 12:07:48 2027 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]:y
    
```

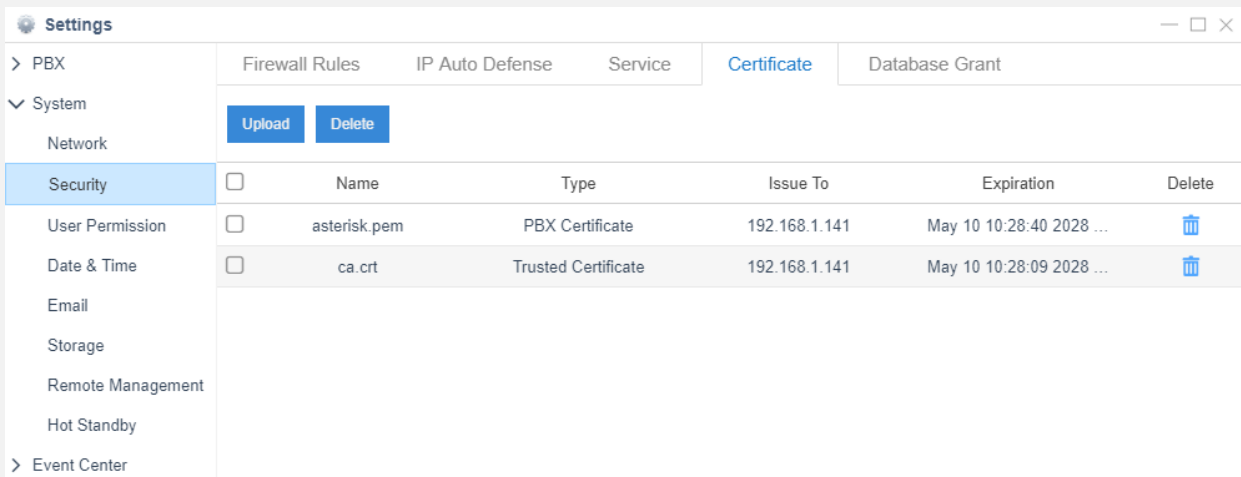
در نهایت فایل client.pem داخل فولدر فعلی ایجاد خواهد شد .
 در حال حاضر شما سه فایل ca.crt و asterisk.pem و client.pem را در اختیار دارید.

گام دوم: بارگذاری certificate در مرکز تلفن

در مرحله‌ی بعد وارد محیط گرافیکی Yeastar شده و مسیر زیر را طی کنید:

Settings > Security > Certificates

در این صفحه روی Upload کلیک کرده و ابتدا Type را روی PBX Certificate گذاشته و فایل asterisk.pem را آپلود نمایید.
 سپس مجدد روی Upload کلیک کرده و Type را روی Trusted Certificate قرار داده و این بار فایل Ca.crt را هم آپلود کنید.
 در نهایت مانند تصویر زیر ۲ عدد فایل آپلود شده خواهیم داشت:

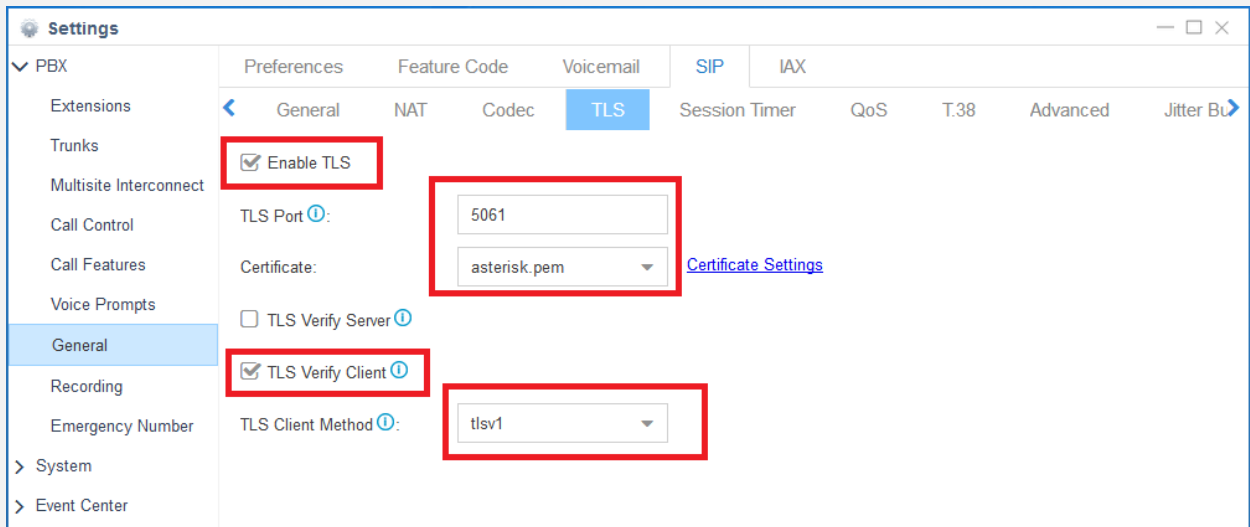


System	Firewall Rules	IP Auto Defense	Service	Certificate	Database Grant
<input type="checkbox"/> Upload <input type="checkbox"/> Delete					
Security	Name	Type	Issue To	Expiration	Delete
<input type="checkbox"/>	asterisk.pem	PBX Certificate	192.168.1.141	May 10 10:28:40 2028 ...	
<input type="checkbox"/>	ca.crt	Trusted Certificate	192.168.1.141	May 10 10:28:09 2028 ...	

در این مرحله نیاز است تا سیستم ری بوت شود.

گام سوم: تنظیمات TLS در مرکز تلفن

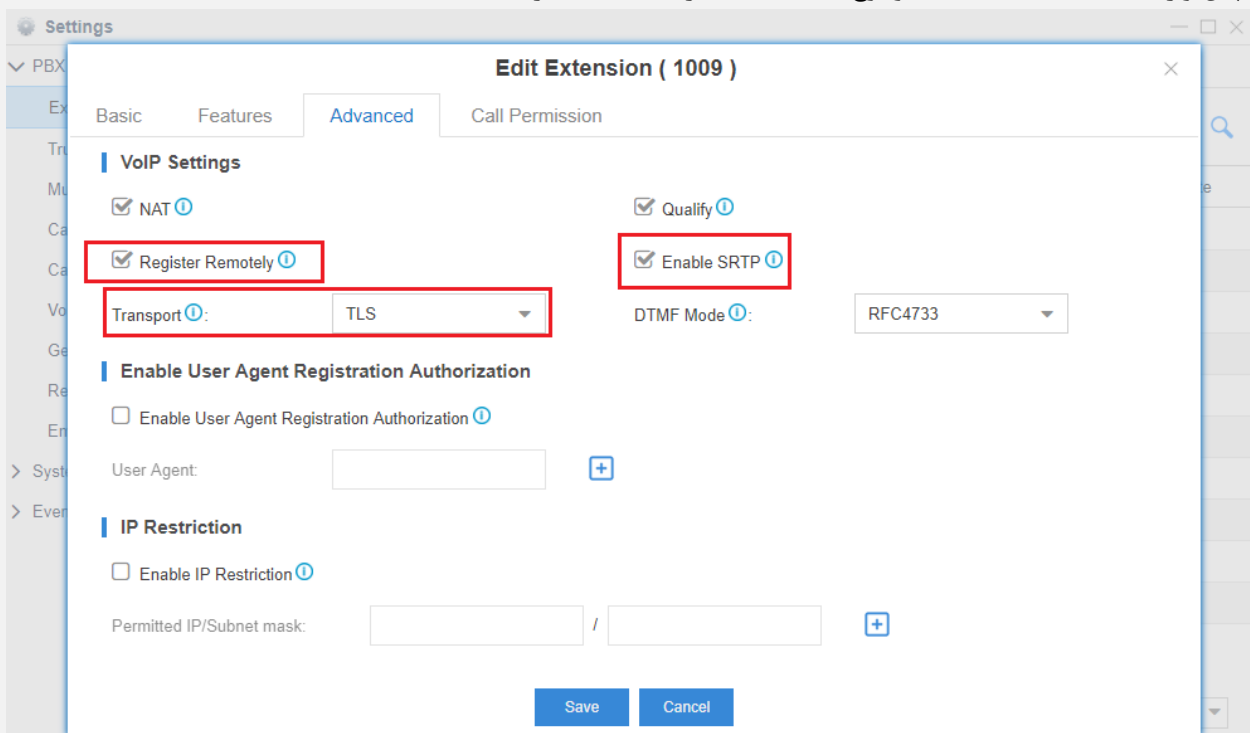
پس از آن راه اندازی مجدد دستگاه وارد مسیر **Settings > General > SIP > TLS** شده و تنظیمات را مانند زیر انجام دهید:



سپس تنظیمات را ذخیره نمایید.

گام چهارم: تنظیمات TLS برای داخلی مورد نظر

برای انجام تنظیمات روی یک Extension وارد مسیر **Settings > Extensions** شده و برای مثال **Extension 1009** را **Edit** کنید. سپس وارد لبه **Advanced** شده و نوع **Transport** را به **TLS** تغییر دهید.



سپس تنظیمات را ذخیره کنید.

توجه: گزینه **register remotely** برای کاربران بیرون از شبکه داخلی می بایست فعال گردد.

توجه: با گزینه **Enable SRTP**، مدیا نیز رمزگذاری می شود.

گام پنجم: تنظیمات داخلی در تلفن Akuvox

پس از تعریف داخلی مورد نظر، وارد محیط گرافیکی پنل تلفن **Akuvox** شوید. از منوی سمت چپ روی **Accounts** و سپس زیر منوی **Basic**، کلیک نمایید.

داخلی مورد نظر که پیش تر در یستار ایجاد شد را در اینجا تعریف کنید:

Akuvox LogOut

▶ Status
 ▼ Account **Basic**
 Advanced
 ▶ Network
 ▶ Phone
 ▶ PhoneBook
 ▶ Upgrade
 ▶ Security

Account-Basic

SIP Account

Status: Registered
 Account: Account 1
 Account Active: Enabled
 Display Label: 1010
 Display Name: 1010
 Register Name: 1010
 User Name: 1010
 Password:

SIP Server 1

Server IP: 192.168.1.63 Port: 5061
 Registration Period: 1800 (30~65535s)

SIP Server 2

Server IP: Port: 5060
 Registration Period: 1800 (30~65535s)

Outbound Proxy Server

Enable Outbound: Disabled
 Server IP: Port: 5060
 Backup Server IP: Port: 5060

Transport Type

Transport Type: TLS

NAT

NAT: Disabled
 Stun Server Address: Port: 3478

Submit Cancel

Help

Note :
 Max length of characters for input box:
 255: Broadsoft Phonebook server address
 127: Remote Phonebook URL & AUTOP Manual Update Server URL
 63: The rest of input boxes

Warning :

Field Description :

Submit Shortcut
 Submit Cancel

همان طور که دیده می‌شود، برای Transport Type TLS و پورت 5061 برای SIP Server 1 که همان آدرس سرور Yeastar می‌باشد، قرار داده شده است. در نهایت تنظیمات را ذخیره کنید. که در این مرحله داخلی شما رجیستر خواهد شد. همچنین برای فعالسازی SRTP داخل تلفن به مسیر Account > Advanced > Encryption روی Compulsory ست کنید:

Broadsoft

AOC: Disabled

Encryption

Voice Encryption(SRTP): Compulsory

NAT

UDP Keep Alive Messages: Enabled
 UDP Alive Msg Interval: 30 (5~60s)
 RPort: Disabled

Warning :

Field Description :

Submit Shortcut
 Submit Cancel

نکته: SRTP تنها در صورتی که هم در سمت سرور و هم در سمت تلفن فعال شده باشد عمل خواهد کرد؛ در صورتی که در یکی از طرفین فعال و در سمت دیگر غیر فعال باشد، تماس برقرار "نخواهد" شد.