

## راه اندازی TLS/SRTP در تلفن های Akuvox و مرکز تلفن FreePBX

یکی از قابلیت هایی که تلفن های تحت شبکه آکووکس پشتیبانی می کنند قابلیت استفاده از TLS به جای UDP برای سیگنالینگ و همچنین SRTP برای امنیت انتقال صدا می باشد.

در این آموزش ما از یک تلفن مدل Akuvox R59P به عنوان کلاینت و از سیستم تلفنی FreePBX 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 زمان نصب FreePBX، یک Certificate به صورت self-signed ساخته شده و به صورت پیش فرض برای تمامی بخش های مورد نیاز، استفاده می شود. بنابراین نیازی به ساخت certificate جدیدی نیست مگر اینکه certificate حذف شده باشد و یا نیاز باشد تا با اطلاعات متفاوت ایجاد شود.

برای ساخت یک Certificate به صورت self-signed در محیط گرافیکی FreePBX، مسیر زیر را طی نمایید:

Admin > Certificate Management

سپس مانند تصویر زیر برای ساخت Certificate اقدام کنید:



**Certificate Management**

What is Certificate Manager?

+ New Certificate - + Generate CSR Import Locally

+ Generate Let's Encrypt Certificate + Upload Certificate + Generate Self-Signed Certificate

Description	Type	Default	Action
No matching records found			

Hover over the 'Default' column and click to make a certificate the system default  
 Note: Making a certificate the 'default' changes certificate settings in Advanced Settings ONLY. It will force said certificate to be the default for options in Advanced Settings that require certificates. It will also place a standard set of the certificate and it's key into /etc/asterisk/keys/integration for use by other applications

و فیلدهای مربوطه را مانند تصویر زیر با مقادیر مورد نظر تکمیل کنید:



**Add New Certificate**

Host Name 192.168.1.63 آی پی فزی پی پی اکس را در این قسمت وارد میکنیم

Description server یک توضیح دلخواه بنویسید

Organization Name SenaTelecom نام دلخواه برای سازمان

Generate Certificate Reset

در پایان با صفحه زیر مواجه خواهیم شد که نشان می دهد certificate مورد نظر ساخته شده است. در صورتی که چندین certificate ساخته شده باشد، می توانید یکی از آن ها را به صورت default انتخاب نمایید.

### Certificate Management

What is Certificate Manager?



Added new certificate

+ New Certificate + Generate CSR **Delete Self-Signed CA** Import Locally

Certificate	Description	Type	Default	Action
192.168.1.63	server	Self Signed		

Showing 1 to 1 of 1 rows

Hover over the 'Default' column and click to make a certificate the system default  
**Note:** Making a certificate the 'default' changes certificate settings in Advanced Settings ONLY. It will force said certificate to be the default for options in Advanced Settings that require certificates. It will also place a standard set of the certificate and it's key into /etc/asterisk/keys/integration for use by other applications

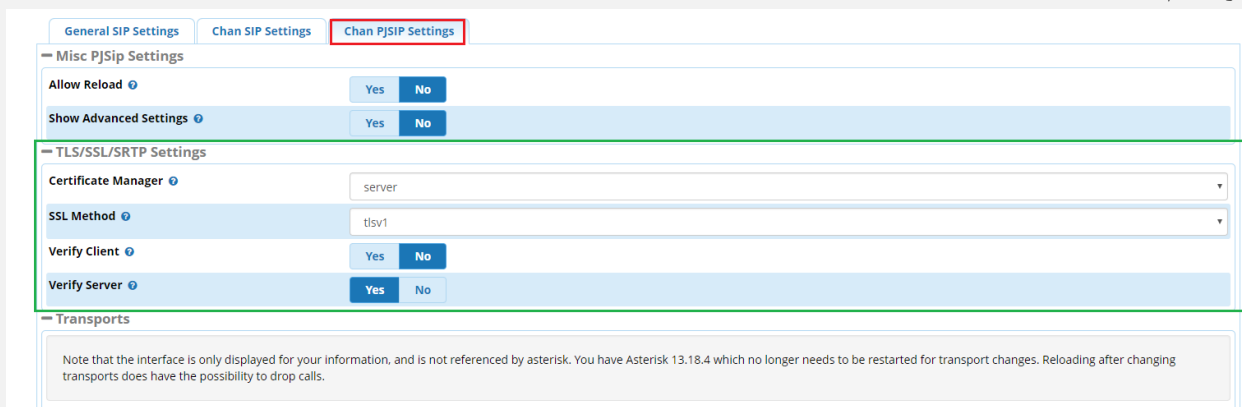



## گام دوم: تنظیمات SIP/TLS در FreePBX

بعد از ساخت certificate لازم است تا TLS را بر روی FreePBX فعال کنید. برای انجام تنظیمات وارد مسیر زیر شوید:

### Settings > Asterisk SIP Setting

در این آموزش از PJSIP استفاده شده است؛ بنابراین روی لبه Chan PJSIP Settings کلیک کرده و تنظیمات بخش TLS را مانند تصویر زیر انجام دهید:

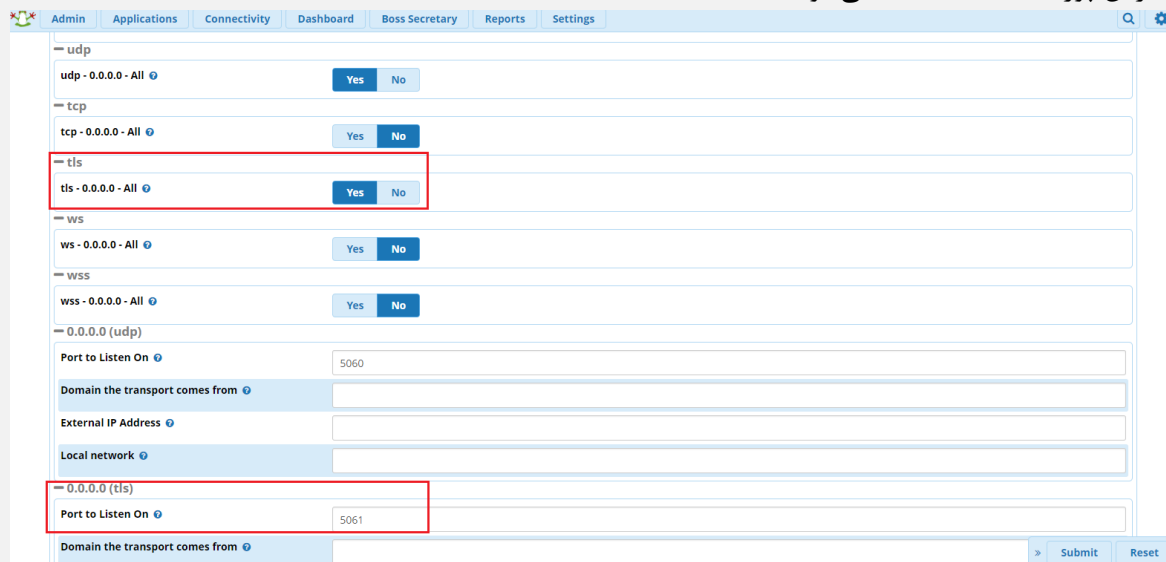


The screenshot shows the 'Chan PJSIP Settings' tab in Asterisk. The 'TLS/SSL/SRTP Settings' section is highlighted with a green box. It includes the following fields:

- Certificate Manager: server
- SSL Method: tlsv1
- Verify Client: Yes
- Verify Server: Yes

همانطور که دیده می‌شود در فیلد ابتدایی، certificate ساخته شده در مرحله قبل انتخاب شده است. تنظیمات مربوط به Verification نیز برای کلاینت بر روی No قرار داده شده که در صورت آپلود Certificate بر روی تلفن، می‌توانید آن را بر روی Yes قرار دهید.

همچنین در همین صفحه در بخش Transport ابتدا TLS را برای PJSIP فعال کرده و سپس یک پورت برای آن در نظر بگیرید که به صورت پیش فرض پورت ۵۰۶۱ استفاده می‌شود.



The screenshot shows the 'Transport Settings' page in Asterisk. The 'tls' section is highlighted with a red box, showing 'tls - 0.0.0.0 - All' with 'Yes' selected. Below it, the '0.0.0.0 (tls)' section is also highlighted with a red box, showing 'Port to Listen On' set to 5061.

### گام سوم: تنظیمات داخلی در FreePBX

حال یک داخلی تعریف کنید که چون در این آموزش از PJSIP استفاده شده است، نوع داخلی را نیز pjsip انتخاب کرده و موارد زیر را در تنظیمات انجام دهید:  
ابتدا در لبه Advanced گزینه Transport را روی TLS انتخاب نمایید:

Send RPID	Send P-Asserted-Identity header
Qualify Frequency	60
<b>Transport</b>	<b>0.0.0.0-tls</b>
Enable AVPF	No Yes

و سپس Media Encryption را روی SRTP قرار دهید:

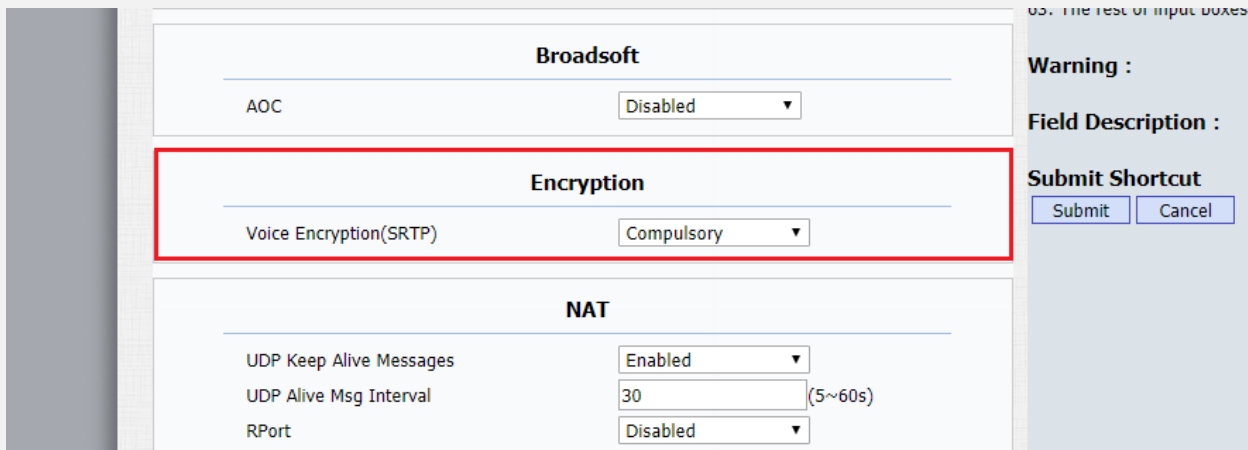
MWI Subscription Type	Auto Unsolicited Solicited
Aggregate MWI	No Yes
<b>Media Encryption</b>	<b>SRTP via In-SDP (recommended)</b>
Session Timers	Yes
Allow Non-Encrypted Media (Opportunistic SRTP)	No Yes

### گام چهارم: 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 FreePBX ایجاد شد را در اینجا تعریف کنید:

همان طور که دیده می‌شود، TLS برای Transport Type و پورت TLS برابر با ۵۰۶۱ برای SIP Server 1 که همان آدرس سرور FreePBX می‌باشد، قرار داده شده است.

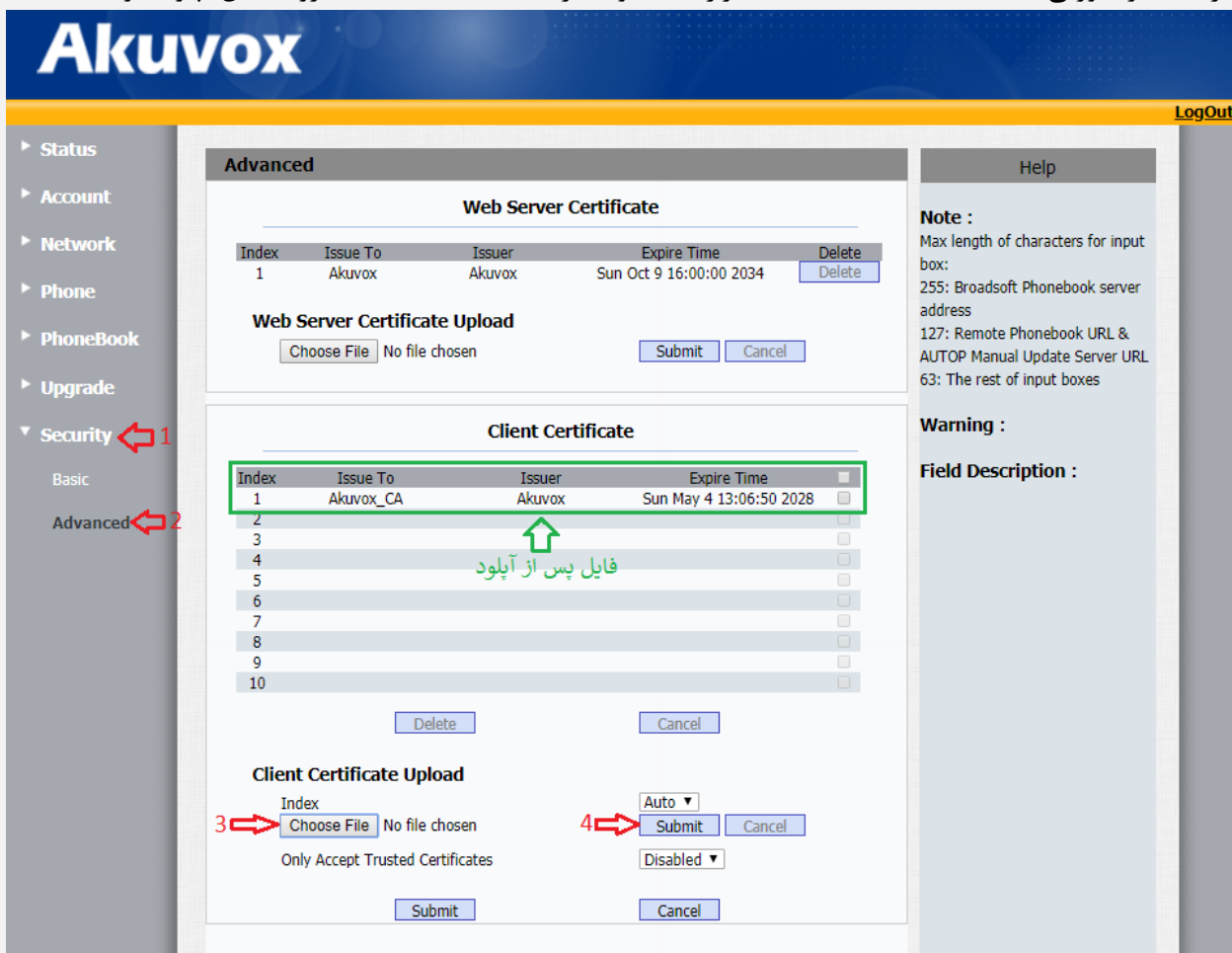
در نهایت تنظیمات را ذخیره کنید. که در این مرحله داخلی شما رجیستر خواهد شد. همچنین برای فعالسازی SRTP داخل تلفن به مسیر Account > Advanced > Encryption رفته و داخل صفحه گزینه Encryption را روی Compulsory ست کنید:



The screenshot shows the Broadsoft configuration interface. The 'Encryption' section is highlighted with a red box, showing 'Voice Encryption(SRTP)' set to 'Compulsory'. Other sections include 'Broadsoft' with 'AOC' set to 'Disabled' and 'NAT' with 'UDP Keep Alive Messages' set to 'Enabled', 'UDP Alive Msg Interval' set to '30', and 'RPort' set to 'Disabled'.

**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.

**نکته:** در حال حاضر در سمت سرور Verify Client=No قرار داده شده و به همین دلیل نیازی به آپلود کردن Certificate در تلفن وجود ندارد. اما در صورتی که Verify Client=Yes قرار داده شود نیاز است تا Certificate روی تلفن آپلود شود.



The screenshot shows the Akuvox web interface. The 'Client Certificate' section is highlighted with a green box. It contains a table with columns: Index, Issue To, Issuer, and Expire Time. The first row is highlighted with a green border and contains the text 'فایل پس از آپلود' (File after upload) with an upward arrow. Below the table are 'Delete' and 'Cancel' buttons. The 'Client Certificate Upload' section has a 'Choose File' button (labeled 3), a 'Submit' button (labeled 4), and a 'Cancel' button. The 'Index' field is set to 'Auto' and 'Only Accept Trusted Certificates' is set to 'Disabled'.