CONFIGURAÇÕES DE SIP TLS

(Xhand)

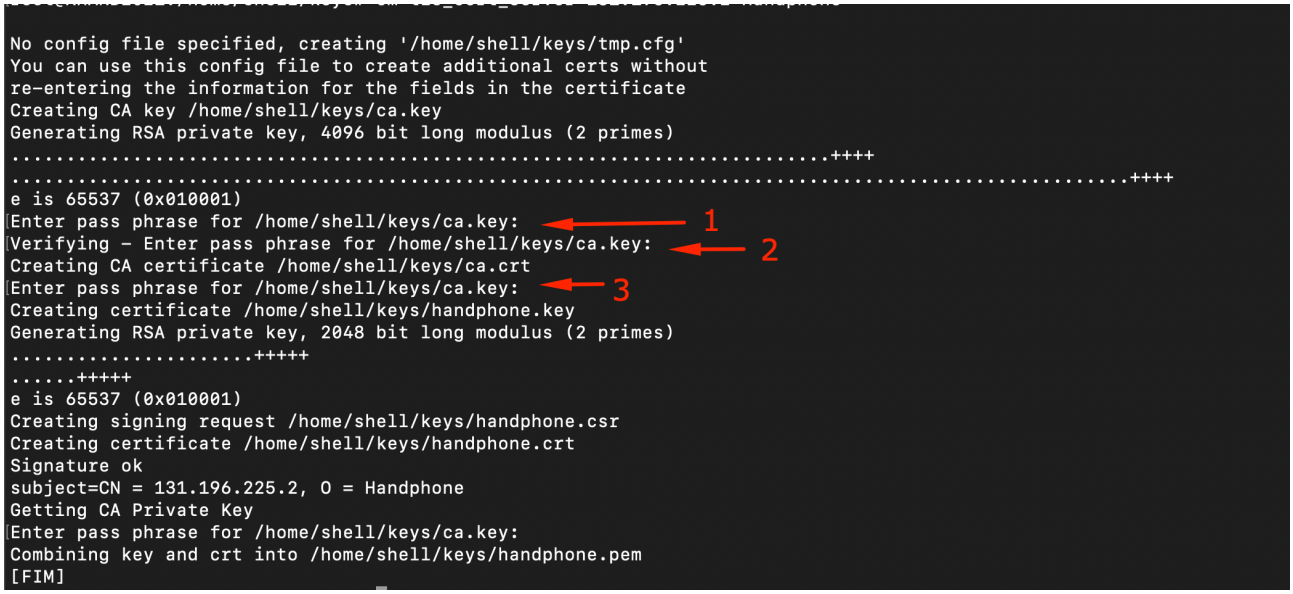
Handphone 2019

PROCEDIMENTO TLS

Esse documento tem por objetivo demonstrar a utilização de endpoints com protocolo SIP utilizando método TLS com certificados gerados pela própria central.

O primeiro passo consiste em configurar os certificados crt e ca dentro do equipamento da Handphone®.

Passo 1)



Executar o seguinte comando: *sudo cm tls_cert_server DNS_OU_HOST Nome_da_Organização (**sem espaços)***

Exemplo: sudo *cm tls_cert_server sip.handphone.com.br Handphone*

A central ira pedir para ser digitado uma chave, importante lembrar dessa chave pois será utilizada no futuro.

Passo 2)

Esse Passo consiste em gerar o certificado para o ramal

Executar o seguinte comando: sudo cm tls_cert_client Nome_da_Organizacao (sem espaços) Ramal

Exemplo: *sudo tls_cert_client Handphone 9301*

```
suporte:~$ sudo cm tls_cert_client Handphone 9301

No config file specified, creating '/home/shell/keys/tmp.cfg'
You can use this config file to create additional certs without
re-entering the information for the fields in the certificate
Creating certificate /home/shell/keys/9301.key
Generating RSA private key, 2048 bit long modulus (2 primes)
.................................+++++
.....................+++++
e is 65537 (0x010001)
Creating signing request /home/shell/keys/9301.csr
Creating certificate /home/shell/keys/9301.crt
Signature ok
subject=CN = xhand, O = Handphone
Getting CA Private Key
Enter pass phrase for /home/shell/keys/ca.key:
Combining key and crt into /home/shell/keys/9301.pem
[FIM]
```

Esse procedimento irá criar o certificado para o ramal 9301.

Para visualizar o certificado acesse a pasta keys, e execute o seguinte comando:
sudo cat 9301.pem

Será necessário copiar o certificado e colocar em um bloco de notas, salvando com o nome 9301.pem (trocar o 9301 pelo ramal que você esta utilizando)

Faça a mesma coisa com o arquivo *ca.crt*

Passo 3)

Configuração da camada de Transporte TLS

É necessário configurar o transporte TLS para que os ramais possam enviar registros, invites utilizando o certificado TLS.

Essa configuração se encontra no arquivo transport.c dentro da pasta etc.

Comandos: sudo vi transport.c

O seguinte bloco deve ser configurado dentro do arquivo.

[transport-tls]
type=transport
protocol=tls
bind=0.0.0.0:5061
cert_file=/home/shell/keys/handphone.crt
priv_key_file=/home/shell/keys/handphone.key
method=sslv23

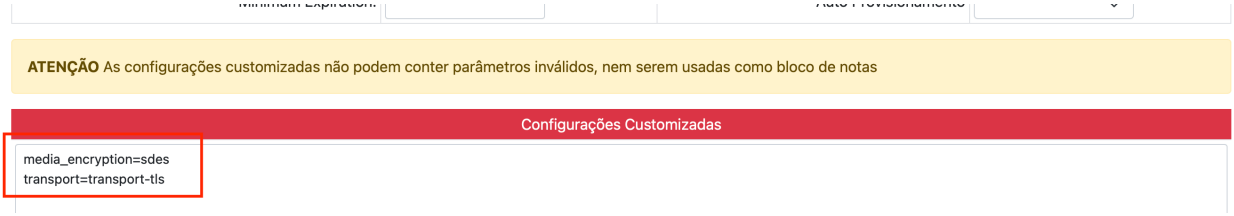
O serviço XHAND deverá ser reiniciado, para saber se as configurações de transporte estão corretas, pode utilizar o comando: sudo cm transport transport-tls

```
Transport:  <TransportId........>  <Type>  <cos>  <tos>  <BindAddress...................>
=============================================================================================

Transport:  transport-tls             tls      0      0  0.0.0.0:5061

 ParameterName              : ParameterValue
 ============================================================
 allow_reload               : false
 async_operations           : 1
 bind                       : 0.0.0.0:5061
 ca_list_file               :
 ca_list_path               :
 cert_file                  : /home/shell/keys/handphone.crt
 cipher                     :
 cos                        : 0
 domain                     :
 external_media_address     :
 external_signaling_address :
 external_signaling_port    : 0
 local_net                  :
 method                     : sslv23
 password                   :
 priv_key_file              : /home/shell/keys/handphone.key
 protocol                   : tls
 require_client_cert        : No
 symmetric_transport        : false
 tos                        : 0
 verify_client              : No
 verify_server              : No
 websocket_write_timeout    : 100
```

Passo 4)

Configurações dos ramais, devemos indicar qual transporte o ramal deverá utilizar e o tipo de encriptação de media.

Na tela de configurações avançadas devemos adicionar o transporte:

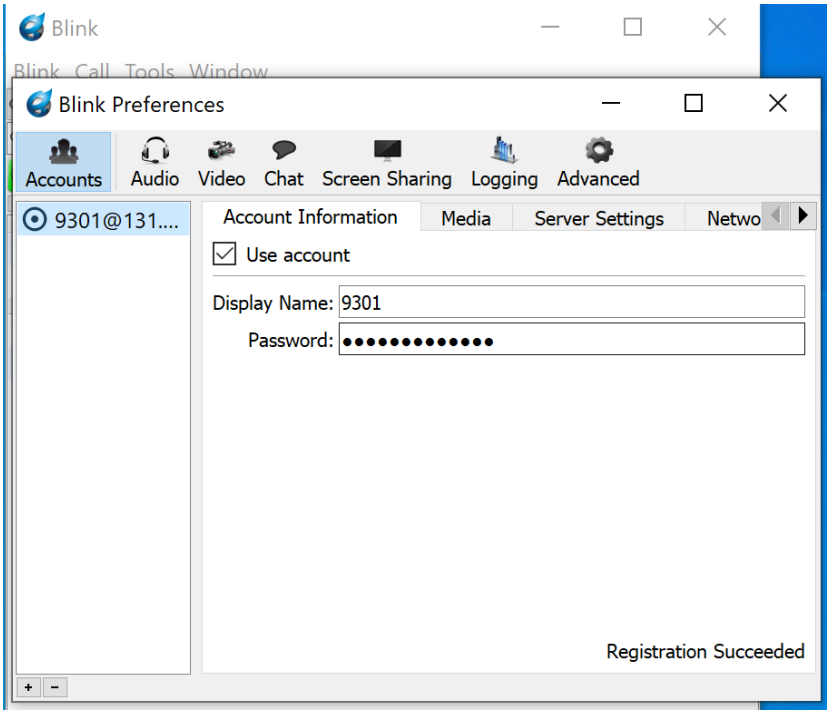


Passo 5)

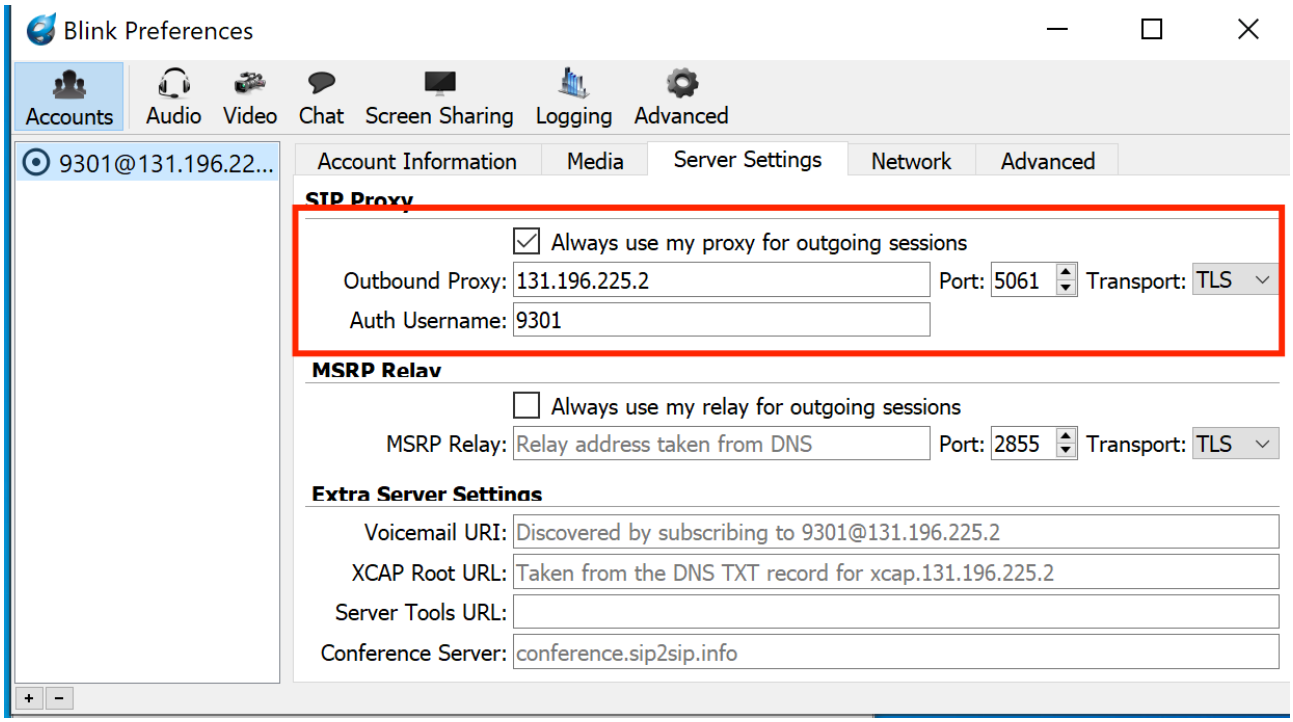
Configuração do Softphone,

Iremos utilizar o softphone blink para os testes:

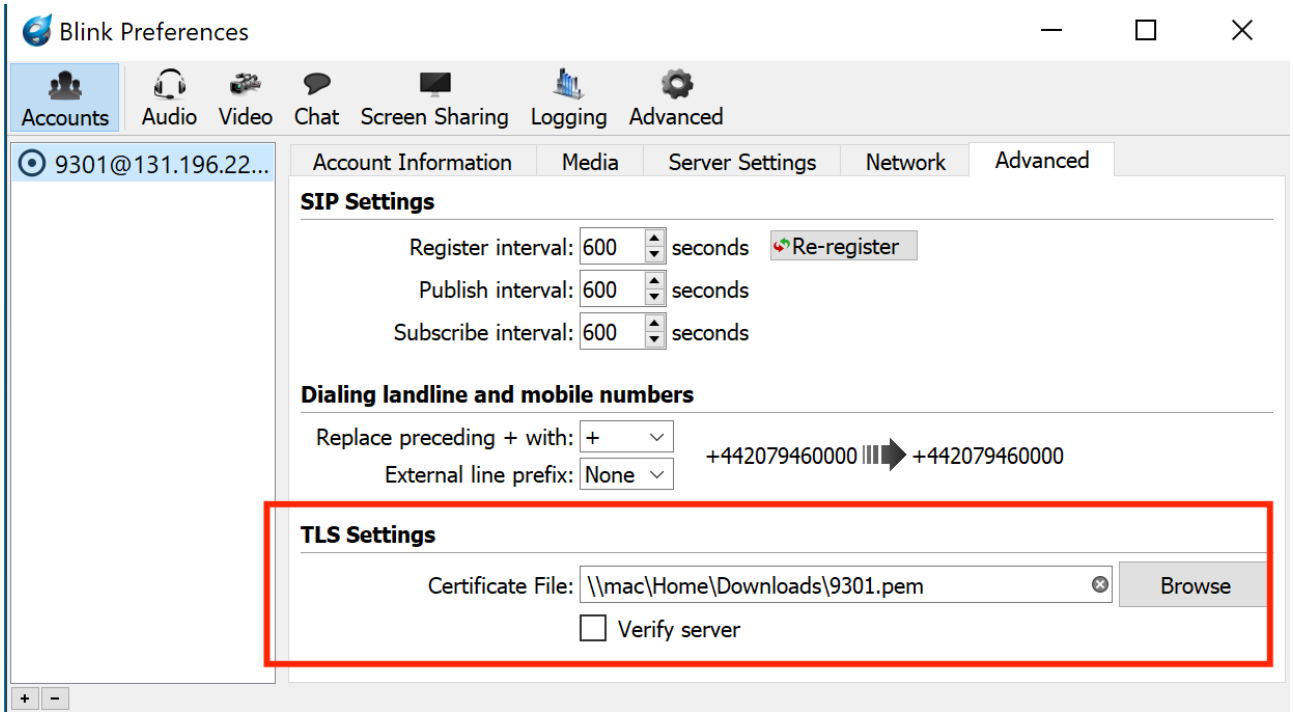
Configure o numero do ramal e senha



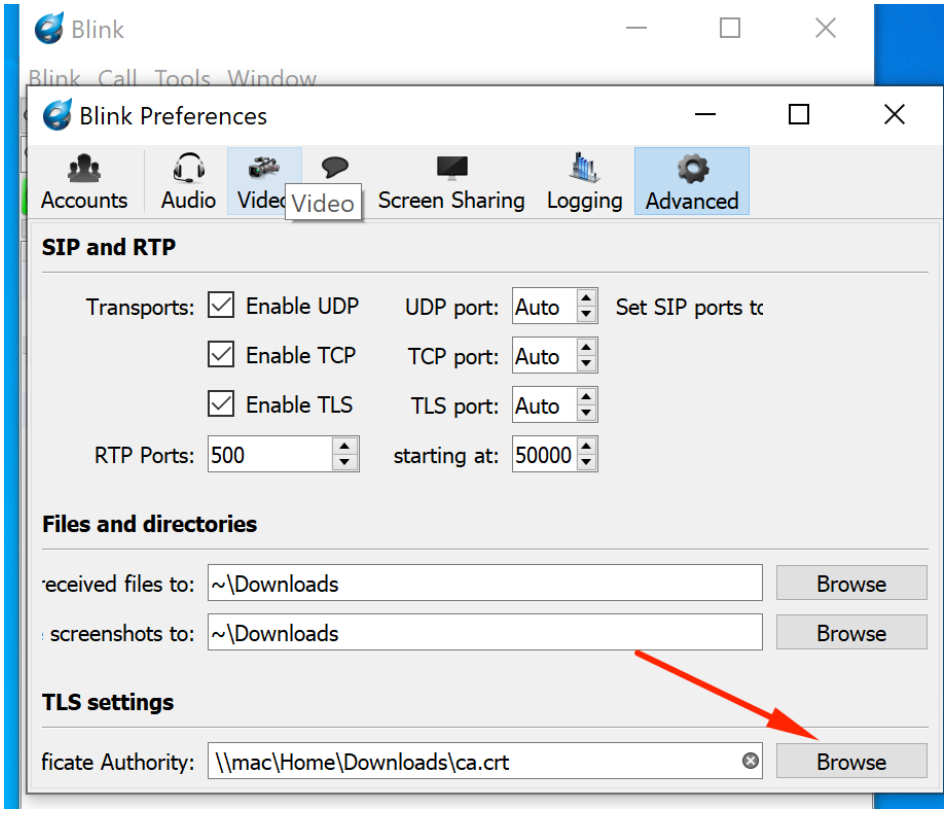
Na Aba Server Settings configure o ip do seu equipamento na porta 5061 e transport TLS



Na aba Advanced coloque o certificado do tipo pem gerado para o seu ramal



Na aba avançadas configure o arquivo TLS do tipo ca.crt



Chamada com TLS ativo

```
<--- Received SIP request (1384 bytes) from TLS:131.196.225.225:53096 --->
INVITE sip:*570@131.196.225.2 SIP/2.0
Via: SIP/2.0/TLS 10.211.55.3:49738;rport;branch=z9hG4bKPj22e70ffff6b84ef5951e3fd2fd2136d6;alias
Max-Forwards: 70
From: "9301" <sip:9301@131.196.225.2>;tag=127155558f394d3dacc00058f503e922
To: <sip:*570@131.196.225.2>
Contact: <sip:20753941@10.211.55.3:49702;transport=tls>
Call-ID: 909b31b86bf94a9286b9644660082577
CSeq: 22168 INVITE
Allow: SUBSCRIBE, NOTIFY, INVITE, ACK, BYE, CANCEL, UPDATE, MESSAGE, REFER
Supported: replaces, norefersub, gruu
User-Agent: Blink 3.2.0 (Windows)
Authorization: Digest username="9301", realm="xhand", nonce="1630938693/56d02019c585a7bc3b32d2ad9a60a533", uri="sip:*570@131.196.225.2", response="c9fefa79f534fcdb0044ebbf0517a1a6", alg
orithm=md5, cnonce="e0e4d050957146b3b707311e19342d3e", opaque="3f5955475310c078", qop=auth, nc=00000001
Content-Type: application/sdp
Content-Length:   508

v=0
o=- 3830916693 3830916693 IN IP4 10.211.55.3
s=Blink 3.2.0 (Windows)
t=0 0
m=audio 50008 RTP/AVP 113 9 0 8 101
c=IN IP4 10.211.55.3
a=rtcp:50009
a=rtpmap:113 opus/48000/2
a=fmtp:113 useinbandfec=1
a=rtpmap:9 G722/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=crypto:1 AES_CM_128_HMAC_SHA1_80 inline:UZdsbFfpVm4LaJKt4dPdUIDI8WZhGeqBFKmuUjTT
a=crypto:2 AES_CM_128_HMAC_SHA1_32 inline:Jdn1/Yg1TLTcxmT9R9YL8hxvW6LHqIVJPB5cnXkL
a=sendrecv
```