Asterisk TLS

配置 Asterisk TLS 传输，以下三个为网络上的教程：

Configuring Asterisk with TLS enabled

SIP TLS Transport

Secure Calling Tutorial

Asterisk 配置

1. 使用 Asterisk 源码中的工具生成 Asterisk 服务器及 SIP Phone 相关的验证文件：

```
mkdir /etc/asterisk/tls
cd /usr/src/asterisk-13.1.0/contrib/scripts/
./ast_tls_cert -C 172.16.200.80 -O "Asterisk Server" -d /etc/asterisk/tls （Asterisk 服务器验证文件）
./ast_tls_cert -m client -c /etc/asterisk/tls/ca.crt -k /etc/asterisk/tls/ca.key -C 172.16.8.180 -O "SIP Device" -d /etc/aster
```

```
[root@localhost ~]# mkdir /etc/asterisk/tls
[root@localhost ~]# cd /usr/src/asterisk-13.1.0/contrib/scripts
[root@localhost scripts]# ./ast_tls_cert -C 172.16.200.80 -O "Asterisk Server" -d /etc/asterisk/tls

No config file specified, creating '/etc/asterisk/tls/tmp.cfg'
You can use this config file to create additional certs without
re-entering the information for the fields in the certificate
Creating CA key /etc/asterisk/tls/ca.key
Generating RSA private key, 4096 bit long modulus
.....................................................................................................++
.....................................................................................................
.....................................................++
e is 65537 (0x10001)
Enter pass phrase for /etc/asterisk/tls/ca.key:
Verifying - Enter pass phrase for /etc/asterisk/tls/ca.key:
Creating CA certificate /etc/asterisk/tls/ca.crt
Enter pass phrase for /etc/asterisk/tls/ca.key:
Creating certificate /etc/asterisk/tls/asterisk.key
Generating RSA private key, 1024 bit long modulus
.........................++++++
........++++++
e is 65537 (0x10001)
Creating signing request /etc/asterisk/tls/asterisk.csr
Creating certificate /etc/asterisk/tls/asterisk.crt
Signature ok
subject=/CN=172.16.200.80/O=Asterisk Server
Getting CA Private Key
Enter pass phrase for /etc/asterisk/tls/ca.key:
Combining key and crt into /etc/asterisk/tls/asterisk.pem
[root@localhost scripts]# ./ast_tls_cert -m client -c /etc/asterisk/tls/ca.crt -k /etc/asterisk/tls/ca.key -C 172.16.8.180 -O
 "SIP Device" -d /etc/asterisk/tls -o 80

No config file specified, creating '/etc/asterisk/tls/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 /etc/asterisk/tls/80.key
Generating RSA private key, 1024 bit long modulus
.............++++++
.............................++++++
e is 65537 (0x10001)
Creating signing request /etc/asterisk/tls/80.csr
Creating certificate /etc/asterisk/tls/80.crt
Signature ok
subject=/CN=172.16.8.180/O=SIP Device
Getting CA Private Key
Enter pass phrase for /etc/asterisk/tls/ca.key:
Combining key and crt into /etc/asterisk/tls/80.pem
```

输入四次密码

输入与上一步相同的密码

2. 配置 SIP 全局参数

```
vim /etc/asterisk/sip.conf
[general]
tlsenable=yes
;tlsbindaddr=0.0.0.0
tlscertfile=/etc/asterisk/tls/asterisk.pem
;tlscafile=/etc/asterisk/tls/ca.crt
;tlscipher=ALL
```

```
;tlsclientmethod=tlsv1
```

```
[general]
tlsenable=yes
tlsbindaddr=0.0.0.0
tlscertfile=/etc/asterisk/tls/asterisk.pem
tlscafile=/etc/asterisk/tls/ca.crt
tlscipher=ALL
tlsclientmethod=tlsv1
```

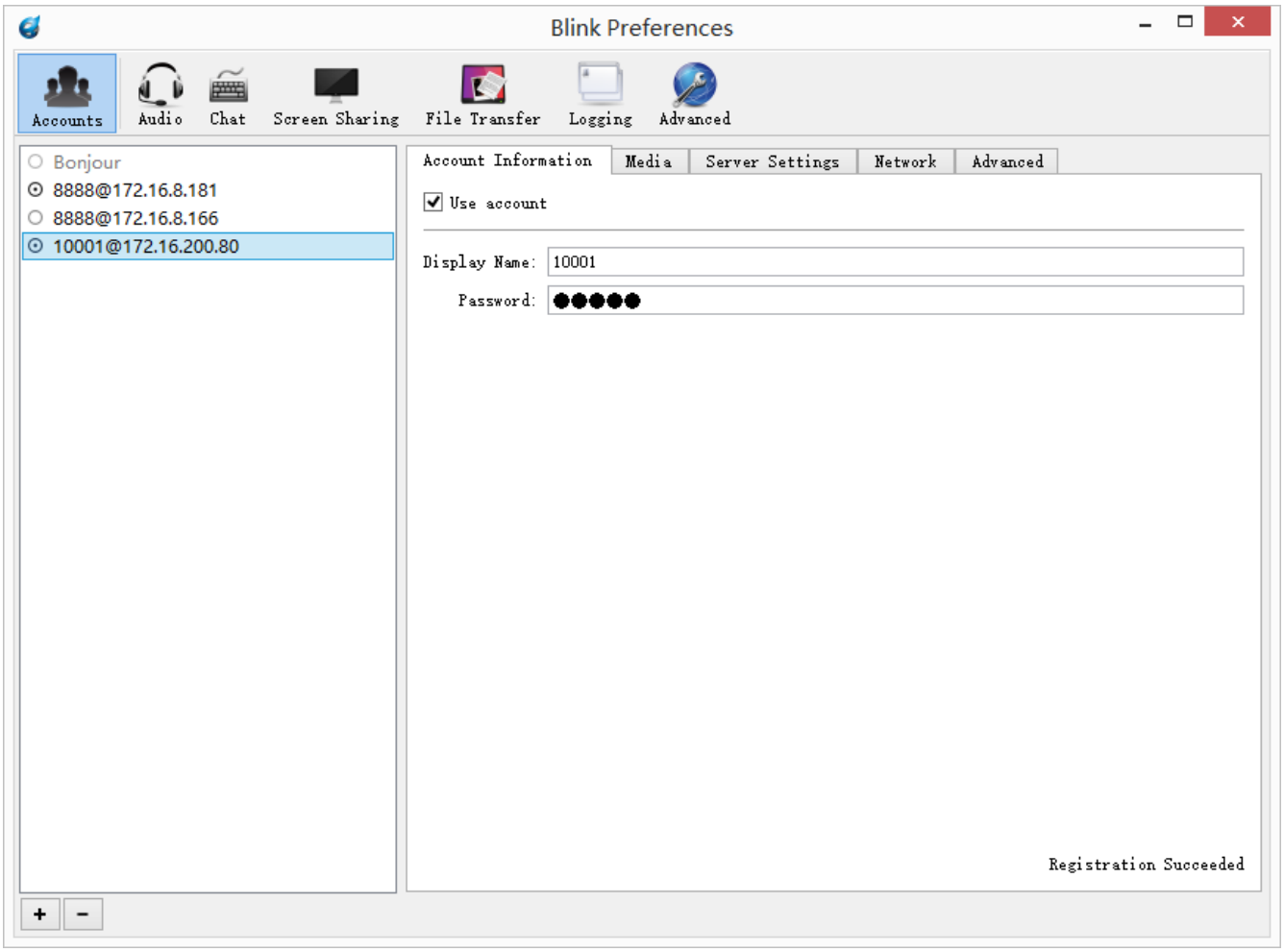
```
3. 配置 SIP 账号
    vim /etc/asterisk/sip_endpoints.conf
    [10001]
    type=friend
    host=dynamic
    username=10001
    secret=10001
    context=from-sip
    transport=tls
    encryption=yes
    disallow=all
    allow=alaw
```

```
[10001]
type=friend
host=dynamic
username=10001
secret=10001
context=from-sip
transport=tls
encryption=yes
disallow=all
allow=alaw
```

SIP 软电话配置

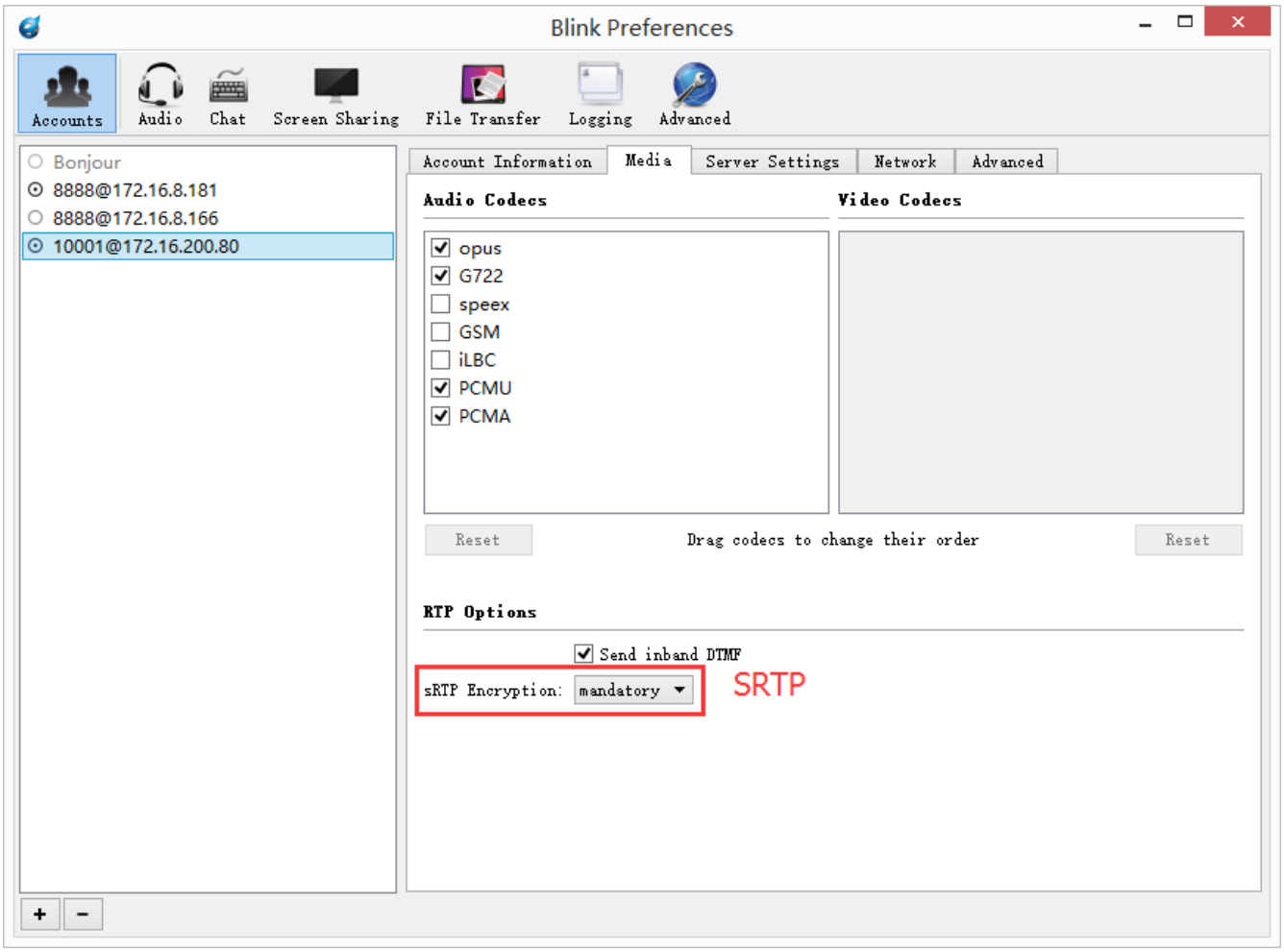
Blink 软电话

```
1. 创建 SIP 账号 10001
```

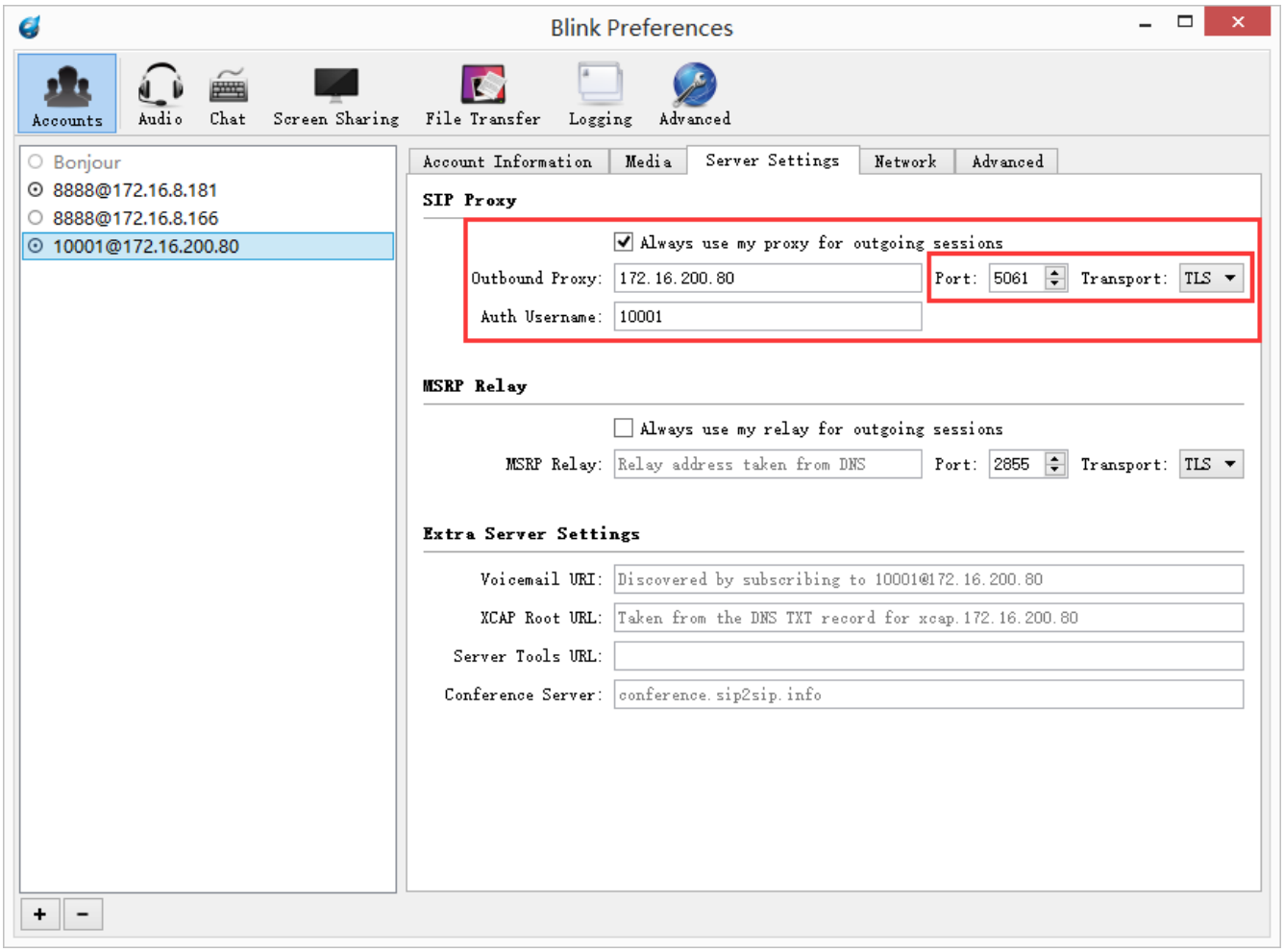


2. 设置 SRTP Encryption，默认为 optional

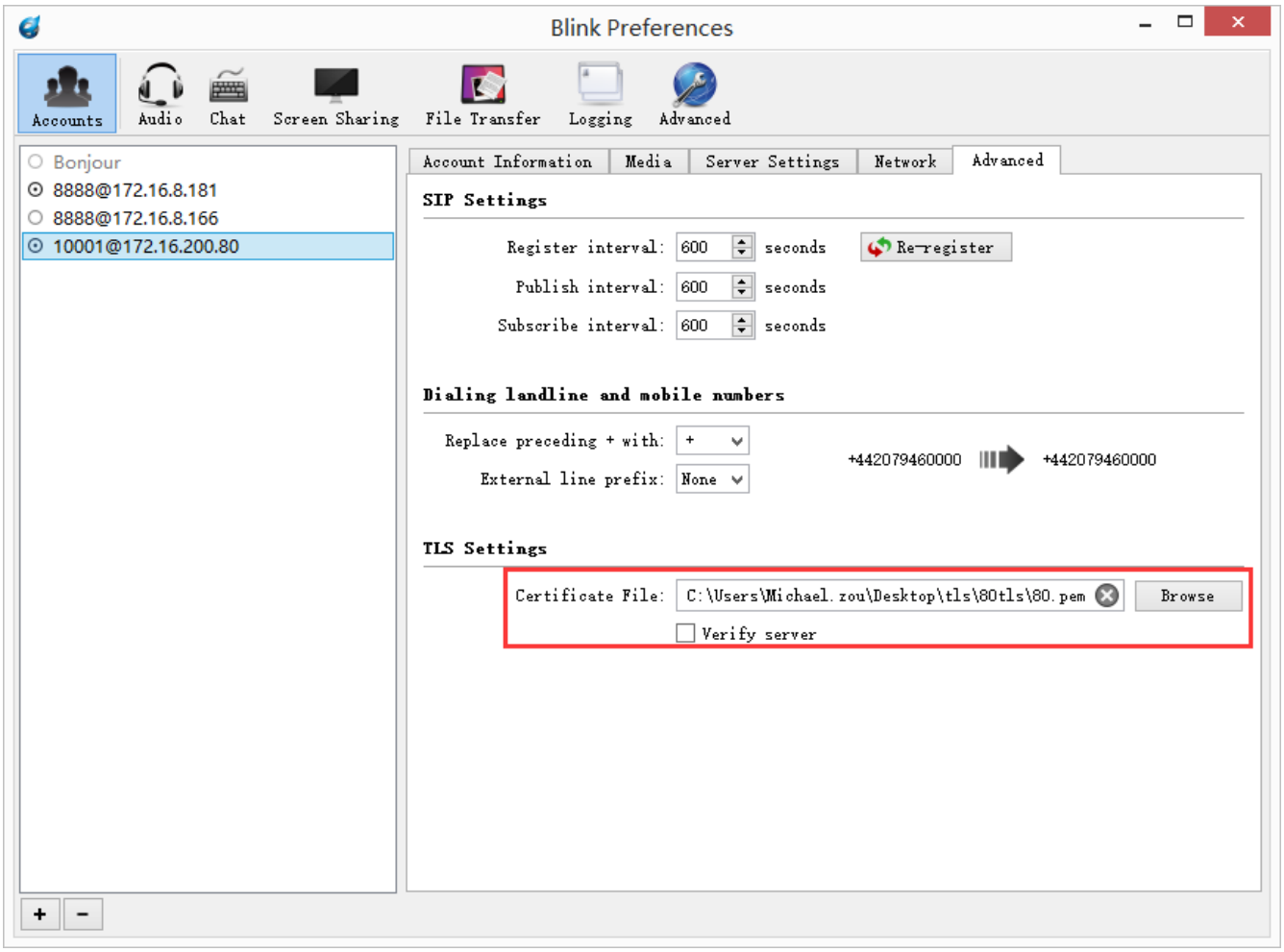
注意：如果 **Asterisk** 的 **SIP** 账号使用了 **encryption=yes**，要将其设为 **mandatory**，且 **asterisk** 必须加载 **res_srtp.so** 模块



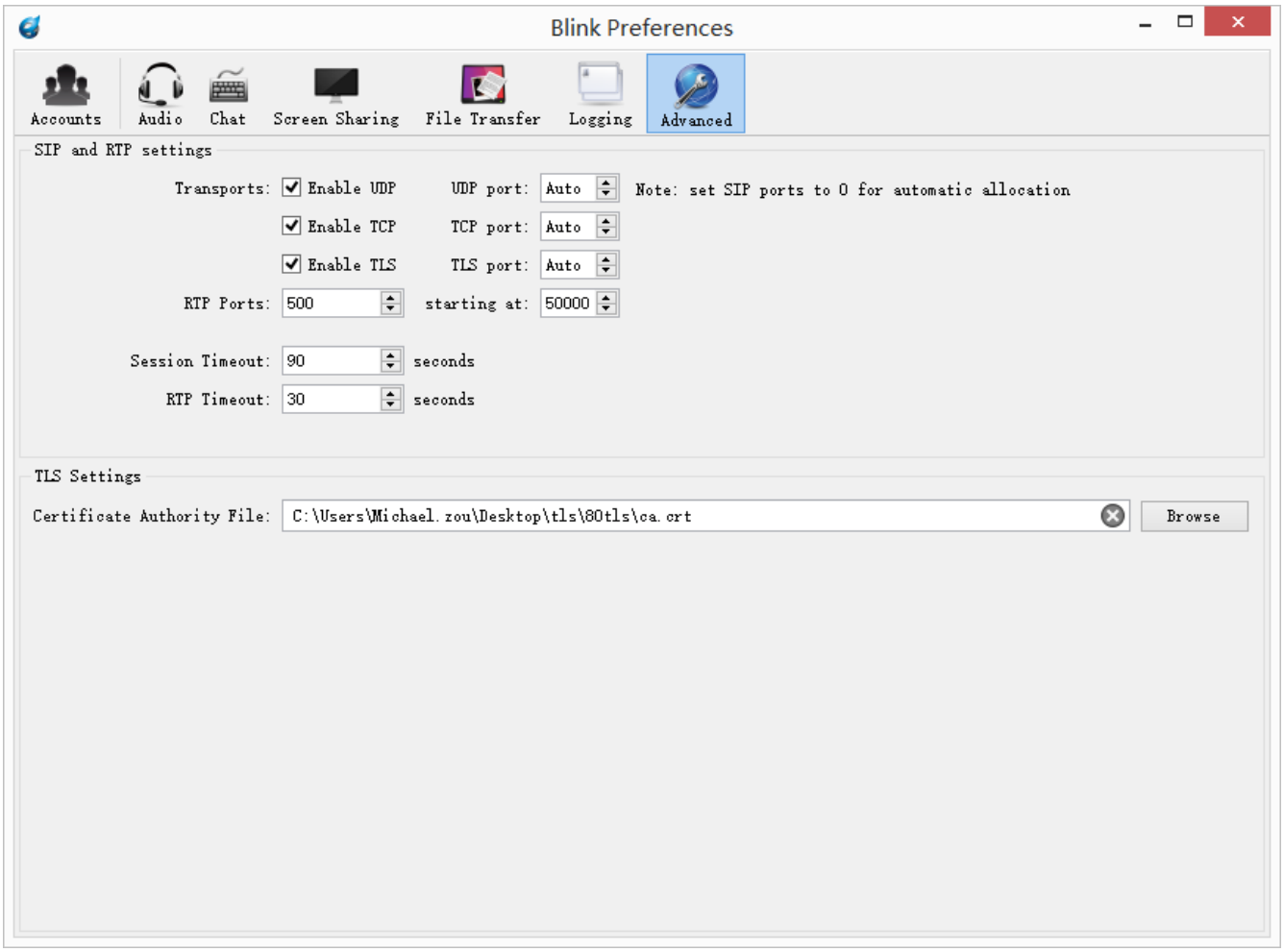
3. 配置对应的服务器，TLS 默认使用 5061 端口



4. 设置 Asterisk 服务器生成的 SIP Phone TLS 验证文件

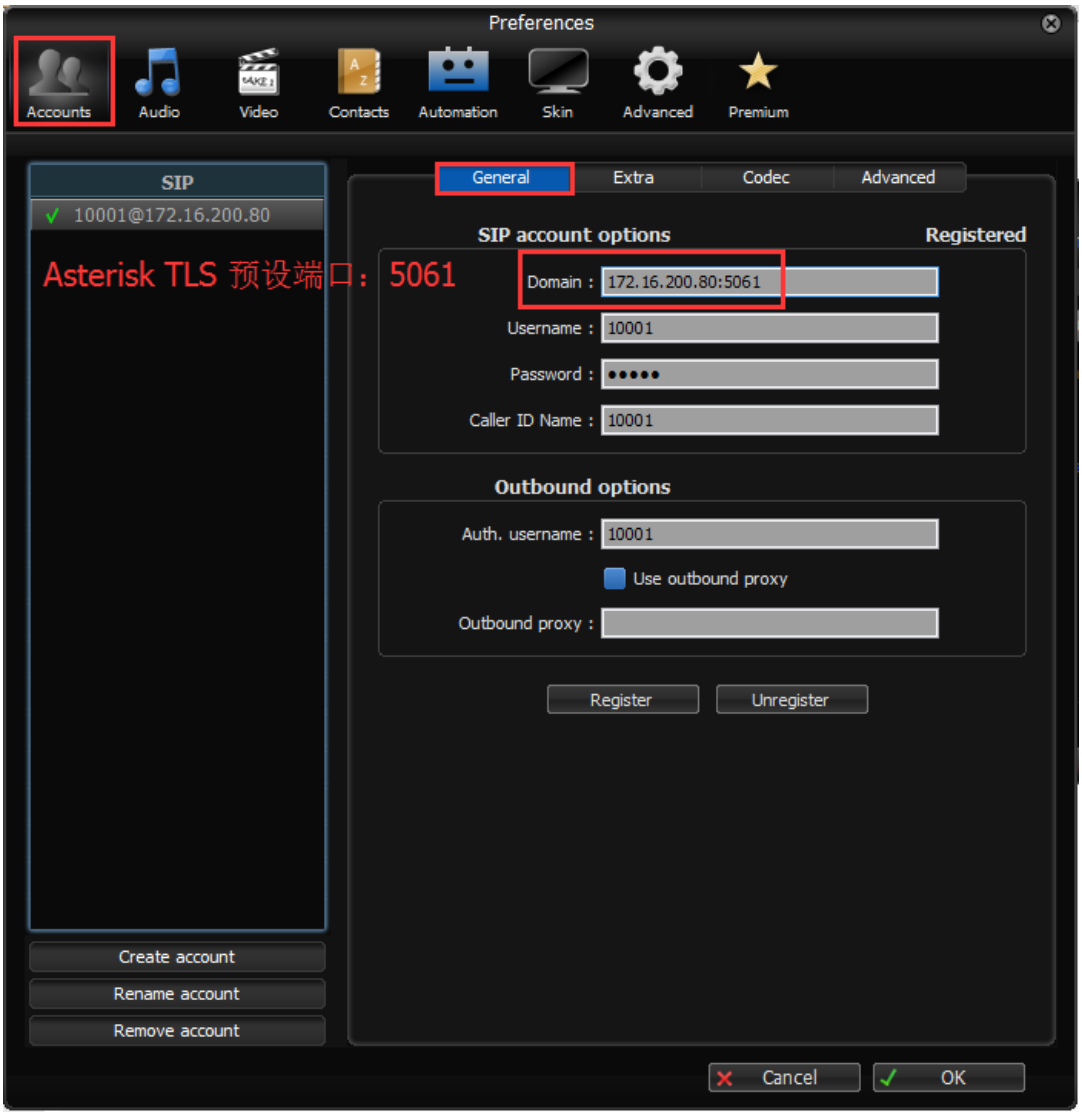


5. 设置 Asterisk 服务器生成的服务器验证文件（可忽略此步骤）

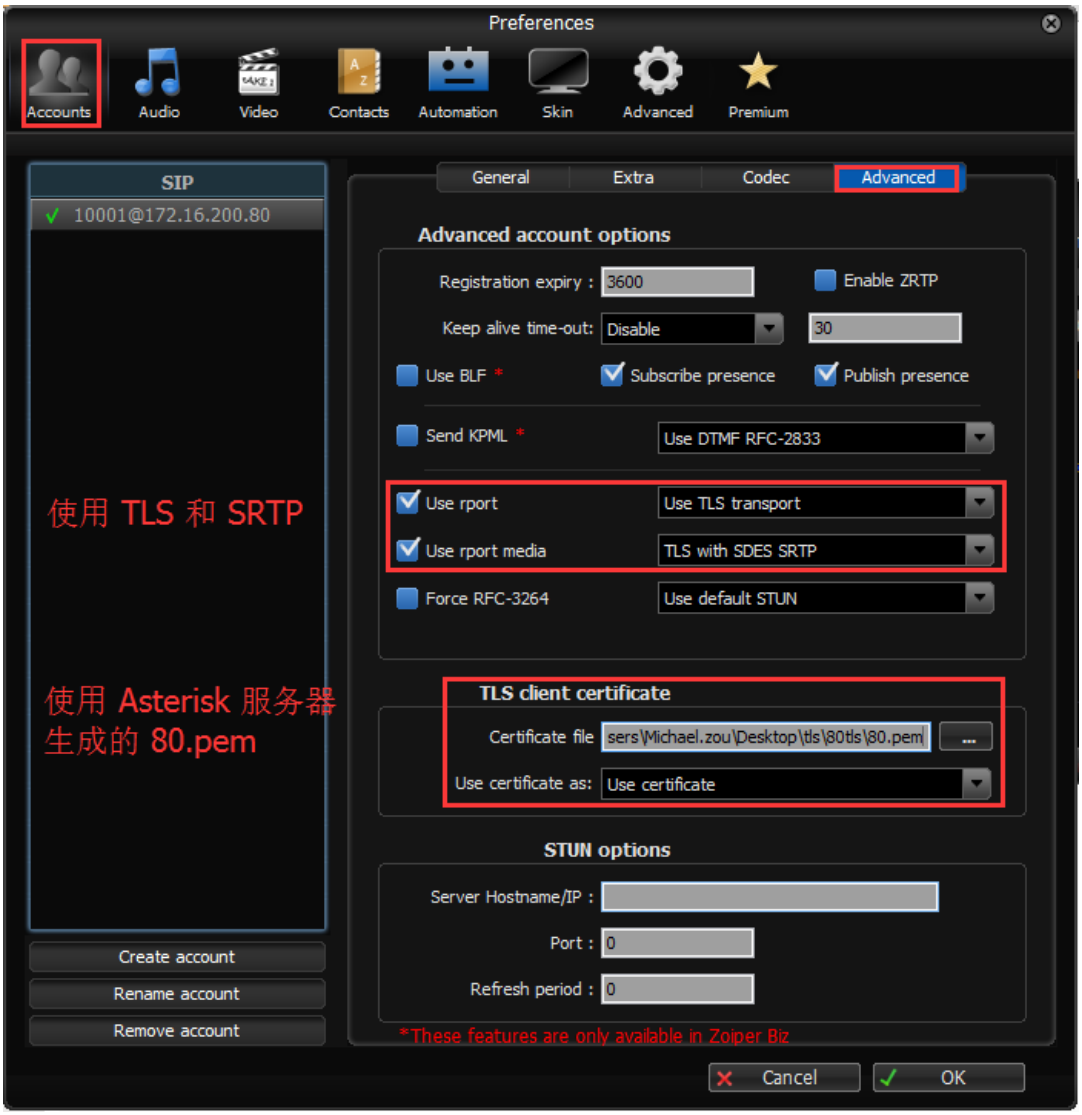


Zoiper 软电话

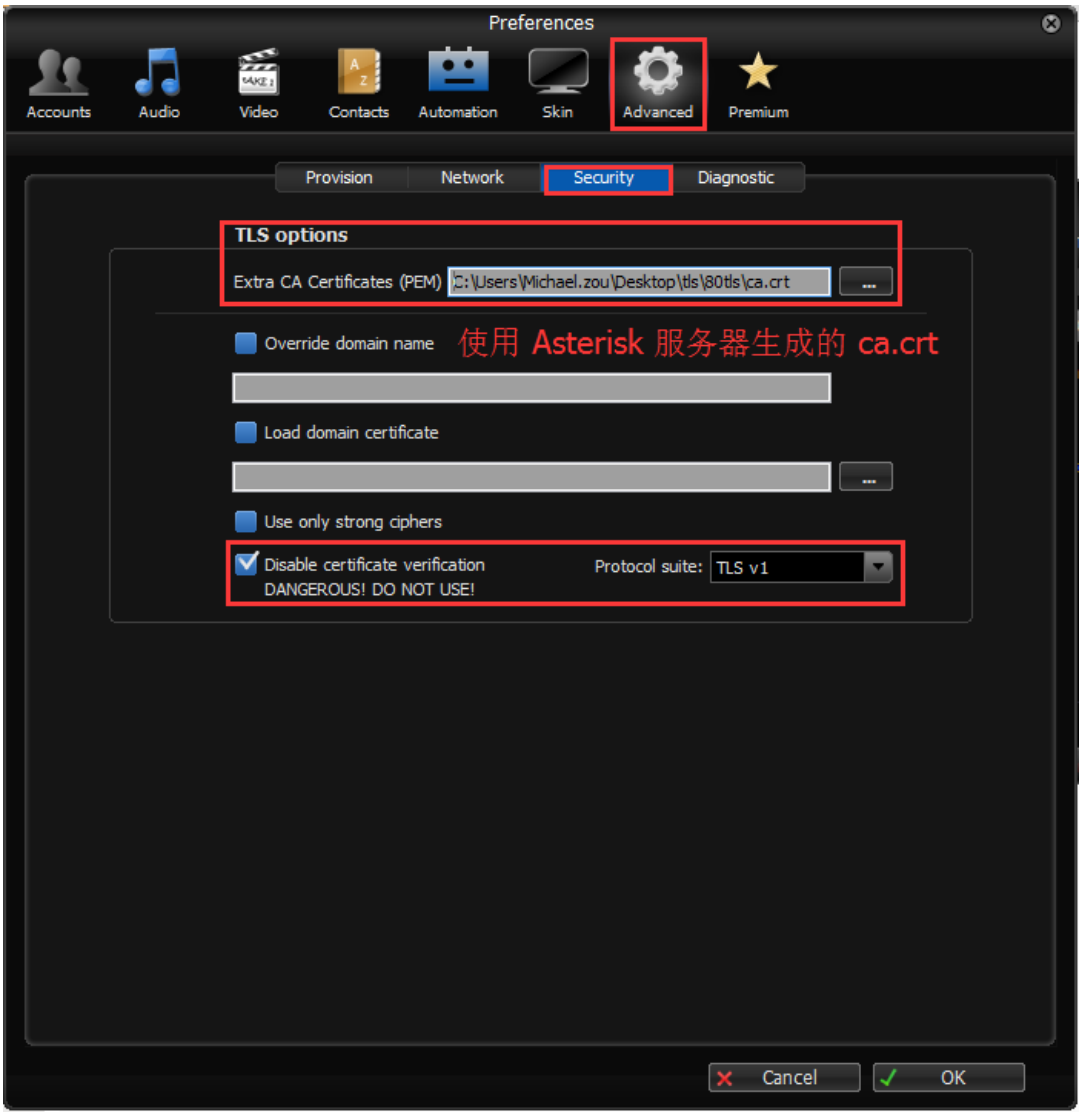
1. 创建 SIP 账号 10001，使用 5061 端口



2. 设置 TLS/SRTP 传输，设置 Asterisk 服务器生成的 SIP Phone TLS 验证文件



3. 设置 Asterisk 服务器生成的服务器验证文件


Preferences
Accounts
Audio
Video
Contacts
Automation
Skin
Advanced
Premium
Provision
Network
Security
Diagnostic
TLS options
Extra CA Certificates (PEM)
C:\Users\Michael.zou\Desktop\tls\80tls\ca.crt
...
Override domain name
使用 Asterisk 服务器生成的 ca.crt
Load domain certificate
...
Use only strong ciphers
Disable certificate verification
DANGEROUS! DO NOT USE!
Protocol suite:
TLS v1
Cancel
OK