# Debugging TLS problems

This page reorganizes the operational steps for **Debugging TLS problems**.

There is a problem with CentOS 9 and TLS with Asterisk. These tools may help to identify the issue

List all the ciphers available

openssl ciphers -v

Check the ciphers available on a SSL server

openssl s_client -connect pbx.mirtapbx.com:5061 -cipher ALL

or using nmap

nmap --script ssl-enum-ciphers -p 5061 pbx.mirtapbx.com

Check the protocols available on SSL server

testssl.sh pbx.mirtapbx.com:5081

To check for the ciphers available on a client, dump the packets with tshark

tshark -i eth0 -w /var/www/html/tls.pcap -s 1500 -f 'host 176.206.10.252 and port 5061'

And then process in wireshark using the ssl.handshake filter. Look for the Secure Socket Layer section

400

Enable LEGACY support

update-crypto-policies --set LEGACY

Check support level

update-crypto-policies --show

In pjsip.conf now you can use

method=tlsv1_2

cipher=DEFAULT,@SECLEVEL=1

# Current Verification

After applying the change, verify the related MiRTA PBX page, the Asterisk logs, and the relevant Status menu entry. Recheck tenant selection before testing tenant-specific behavior.

---

Revision #3
Created 2026-06-02 21:59:16 UTC by Admin
Updated 2026-06-02 22:00:18 UTC by Admin