

StartSSL wss?



DEPRECATED

Webitel 3.1: [StartSSL](#) [wss](#)

SSL www.startssl.com



StartSSL.

(demo-srv.webitel.com) Private Key, Certificate [Class 1 Intermediate Server CA](#).

1. /opt/webitel/certs
2. Private Key /opt/webitel/certs/wss.key
3. Certificate /opt/webitel/certs/wss.crt
4. Class 1 Intermediate Server CA: wget <https://www.startssl.com/certs/sub.class1.server.ca.pem>

webitel

1. pfx webitel:

```
openssl pkcs12 -export -in wss.crt -inkey wss.key -out certificate.pfx -certfile sub.class1.server.ca.pem
```

2. certificate.pfx webitel : /opt/webitel/srv/Webitel.EventWebSocket.addin

Webitel.EventWebSocket.addin

```
<section name="config">
  <set type="setup" name="listen-ip" value="Any"/>
  <set type="setup" name="listen-port" value="6871"/>
  <set type="setup" name="max-connect-count" value="100"/>
  <set type="setup" name="max-request-length" value="100000"/>
  <set type="setup" name="json-format-indent" value="true"/>
  <set type="setup" name="security" value="tls"/>
  <set type="setup" name="certificate" value="/opt/webitel/certs/certificate.pfx"/>
  <set type="setup" name="password" value="itsferapass1"/>
</section>
```

3. webitel
4. , c :

```
openssl s_client -showcerts -connect demo-srv.webitel.com:6871
```

:

```
CONNECTED(00000003)
depth=0 C = UA, CN = demo-srv.webitel.com, emailAddress = chuchko@it-sfera.com.ua
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 C = UA, CN = demo-srv.webitel.com, emailAddress = chuchko@it-sfera.com.ua
verify error:num=27:certificate not trusted
verify return:1
depth=0 C = UA, CN = demo-srv.webitel.com, emailAddress = chuchko@it-sfera.com.ua
verify error:num=21:unable to verify the first certificate
verify return:1
---
```

```
0 s:/C=UA/CN=demo-srv.webitel.com/emailAddress=chuchko@it-sfera.com.ua
   i:/C=IL/O=StartCom Ltd./OU=Secure Digital Certificate Signing/CN=StartCom Class 1 Primary Intermediate
Server CA
-----BEGIN CERTIFICATE-----
```

MIIGRjCCBS6gAwIBAGIDEyL6MA0GCSqGSIB3DQEBCwUAMIGMMQswCQYDVQGEwJjTDEWMBGQA1UEChMNU3RhcncRDb20gTHRKLjErMCKGA1UECnMiU2VjdxJlIERPZz10YWwgQ2VydGlmawNhdGUGU2LnbmluZzE4MDYGA1UEAxMVU3RhcncRDb20gQ2xhc3MgYSSwCmlltYXJ5IEludG9ybWJwKwF0ZSB7ZTJZXXIwQGEHhcnMTQW0t1MTQWNTI1aWhcnMTQW0t1MSDcxNjQwYVJBMUQsQ2VQDVQGEwJ3QTEdMBSGA1UEAwMzZGVtby1zcnyud2ViaXRlBc5jb20xJjAkBgkqhkiG9w0BCQEWF2NodWNoa29AaXQtc2Z1cmEY29tLnVhMIIb1jANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAWTmgeZ3ocsZHo817L2daXldo0MNNW5XKp+84Aa+Gvu5ens1mtEm+Lyx7oY0AS9CQVrCq0FK0i9FZ7jwktKBKLXNoYB7pZ3bYqWsqTmmG1hdLaiL4VGLiPqFLsdny0nrJp4i+nA9SUDZMCLYj1ahLV3EGTdpdqbD4nfouYr+5QPSpk5Te862YHHqyEXgppmMpyHRqjZnofeYrbGoIilMIxmb1a0a3YIn0Ksxc0xpJTPg0T+Jwlv0mm5n+YP/ZcCz25cz+A5mUDG13/u31zyRlBN0iyawHzhvJ5z8azJw3wm4H1w//jGQv1ougVpNpX4jIrj45JDglibmccwIDAQBA04IC5jCJCAUwCQYDVDR0TBIAwADALBgNVHQ8EBAMCA6gwEwYDR01BAwwCgYITkYBBQUHAEwHQYDVRO0BbYEFB87Dw/AepywkYwmbP51j4d14HXMB8GA1UdIwYQMABaF0Q0CNCCYsKuf9BtrCPFMZC7VdixFMcWGA1UdEQQLMCOCFGRlBw8tc3J2Lnd1Yml0ZWwuY29tggt3ZWJpdGVsLmNvbTCCAAYGA1UdIASCAU0wggFJMAgGBmeBAEATCCATsG6cysGAQQggbu3AQIDMIIBKjAuBggrBgEFBQcCARYiaHR0cDovL3R3c3dy52bG9ydG9yYHNzBc5jb20vcG9sawN5LNRk3ZjCB9yIKwYBBQUHAGIwXoXmGJxYQ2U3dHcnRDb20gQ2VydGlmawNhdGUGU2LnbmluZzE4MDYGA1UEAwMzZGVtby1zcnyud2VydGlmawNhdGUGU2FzIGZlc3VlZCBhY2NvcnRpbmcdG8gdGhLIENSXYNzIDEGVmFsaWRhdGlvbiByZXFlaXJlbWVudHMgb2YgdGh1IFN0YXJ0Q29tIENBIHBvbGJleSwgcWVsawFuY2Ugb25seSmb3tgdGh1IGU2UwZGVkIHB1cnBvc2Ugaw4gY29tcGxpYw5jZSBvZiBoaGUgcWsewluZyBwYXN5I0eSBvYmxpZ2F0aw9ucy4wNQYDVRO0BC4wLDAQoCigYjQyKAHR0cDovL2NybyCSzDGFydHNzBc5jb20yY3J0MS1jcmwUy3J3SMIG0BggrBgEFBQcCBAQSBGtB/MDKGCCSGAQUBZABhi1odHRw0i8vb2Nzc2DGFydHNzBc5jb20vc3ViL2NsYXNzMS9zZXJZXXIvY2EwQgYIKwYBBQUHMAKGNmh0dHA6Ly9haWEuc3RhcncRzc2wUy29tL2NL3dnR3L3N1Yi5jbgFzc2Euc2VydmlmLmNhlNmLhLnDdAJBgNVHR1EHDAaahhhodHRw0i8vd3R3L3N0YXJ0c3NsLmNvbS8wDQYJKoZIhvcNAQELAQQDEBAQEBAJE2K20fda4eZK7wkL2QShpa3AQtAr1MBTIOsn5CiD0al7fBGH14cnuNeuqSunchjCga+HcBxaI0b1l8X3iq7ATCoD0M0GRSWePZoxandN4FunAei7A4mfWszjPpTfXZo8aagN8xTN99KEHJPMxfPyvXuXVhZVlp7ibfryjwyF5RPKbRqP+HSEkirF27bnZ8P1AfW5Lkmw150vb6p6+aN5R32Bk0aig3reZqWfSTUpSjA8Tp8GHPubIoZ0IiYfA9y0E2ztPSGBLRDKfJ5D+onK2okoIj50FU70c0YR4equH2VwkTYcykYw6X6TAOR1E5CSReYgKTHKUN7nnfYzJyna0=

```
subject=/C=UA/CN=demo-srv.webitel.com/emailAddress=chuchko@it-sfera.com.ua
issuer=/C=IL/O=StartCom Ltd./OU=Secure Digital Certificate Signing/CN=StartCom Class 1 Primary Intermediate
Server CA
```

```
Protocol   : TLSv1
Cipher     : AES256-SHA
Session-ID:
Session-ID-ctx:
Master-Key: 3819079D8181F4624ABB65F2CD0D6F6842F93AF4670DF63486297010B6C6AB72EC508DF591D23596A976E4C2C4FF98B9
Key-Arg    : None
Krb5 Principal: None
PSK identity: None
PSK identity hint: None
Start Time: 1411737613
Timeout    : 300 (sec)
Verify return code: 21 (unable to verify the first certificate)
```

```
read:errno=0
```

WebRTC

1. pem FreeSWITCH:

```
cat wss.crt wss.key sub.class1.server.ca.pem > wss.pem
cp wss.pem dtls-srtp.pem
```

2. wss.pem FreeSWITCH : /opt/webitel/switch/conf/sip_profiles/internal.xml

```
<param name="tls-cert-dir" value="/opt/webitel/certs"/>
<param name="wss-binding" value=":7443"/>
```

- ### 3. FreeSWITCH

4. :

```
openssl s_client -showcerts -connect demo-srv.webitel.com:7443
```

•

```
CONNECTED(00000003)
depth=2 C = IL, O = StartCom Ltd., OU = Secure Digital Certificate Signing, CN = StartCom Certification Authority
verify return:1
depth=1 C = IL, O = StartCom Ltd., OU = Secure Digital Certificate Signing, CN = StartCom Class 1 Primary Intermediate Server CA
verify return:1
depth=0 C = UA, CN = demo-srv.webitel.com, emailAddress = chuchko@it-sfera.com.ua
verify return:1
---
Certificate chain
 0 s:/C=UA/CN=demo-srv.webitel.com/emailAddress=chuchko@it-sfera.com.ua
   i:/C=IL/O=StartCom Ltd./OU=Secure Digital Certificate Signing/CN=StartCom Class 1 Primary Intermediate Server CA
-----BEGIN CERTIFICATE-----
MIIGRjCCBS6gAwIBAgIDEyL6MA0GCSqGSIb3DQEBCwUAMIGMMQswCQYDVQQGEWJJ
TDEwMBQA1UEChMNU3RhcnRDb20gTHRkLjErMCkGA1UECxMiU2VjdXJlIERPZ2l0
YWwgQ2VydgLmaWNhdGUgU2lnbmLuZzE4MDYGA1UEAxMvU3RhcnRDb20gQ2xhc3Mg
MSBQcmllYXJ5IEUludGVybWwkaWFOZSBTZjJ2ZXIgaQ0EWWhcNMTQWOTI1MTQWNTI4
WhcNMTUwOTI3MDcxNjQwWjBUMQswCQYDVQQGEWJVQTEdMBsGA1UEAxMUZGVtby1z
cnYud2ViaXRlbC5jb20xJjAKBgkqhkiG9w0BCQEF2NodWNoa29AAXQtC2ZlcmEu
Y29tLnVmHmIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAwTVmgeZ3ocsZ
Ho817L2AdxDldoOMNWy8XKP+8A4a+Gvu5ens1mtEm+Lyx7oY0AS9CQvCrq0FK0i0F
Z7jwkTKBKLN0yB7PtZJBYSQSoqTmmG1hxdLailLv4GliPqFlsdny0nrJP4i+nA9sU
ZDMCLyj1ahLV3eGTGdpqbWdf4nkouYR+5QPspk5xTe8e62YHHqyeXQgypMpPyHRq
jZnoFeYrbGoIilMXibmla0a3YIn0Ksxc0xpJTpg0T+JwlV0mm5n+YP/ZcCz25cz+
A5mUDG1J/u3izyRLBN0iywaHzhvJ5z8azJw3wm4H1w//jGQvlougVYPnx4jIrj45
JDglibmcwIDAQABO4IC5JCcAuIwCQYDVR0TBAlWADALBgNVHQ8EBAMCA6gewEYD
VR0lBAwwCgYIKwYBBQUHAWEwHQYDVR00BBYEFF8jDw/AEpykWYmbPf5lj0Lt4HX
MB8GA1UdIwQYMBAAFOtCNncySkuF9BtrCPfMZC7vdixFMCwGA1UdEQQLMCOCFGRl
bw8tc3J2Lndlym10ZWwuY29tggt3ZWJpdGVsLmNvbTCCAUYGA1UdIASCAU0wggFJ
MAGGBmeBDAECAATCATSGCysGAQQBgbu3AQIDMIIIBKjAUBggrBgEFBQCcARYiaHR0
cDovL3d3dy52dGFydHNzbc5jb20vcG9saWN5LnBkZjCB9wYIKwYBBQUHAgiGeow
JxyGU3RhcnRDb20gQ2VydgLmaWNhdGLvbiBBdXRob3JpdHkwAWIBARqBvLRoaXMg
Y2VydgLmaWNhdGUgd2FzIGlzczVLZCBhY2NvcmlRpbmcgdG8gdGhlIENsYXNzIDEG
VmFsawRhdlGlvbiByZXFaXJlbWVudHMgb2YgdGhlIFN0YXJ0Q29tIENBIHBvbGlj
eSwgcmlVsawFuY2Ugb25seSBmb3IgdGhlIGludGVuZGVkIHBIbnBvc2Ugaw4gy29t
cGxpYwQ5jZSBviB0aGUgcmlwsewluZyBwYXJ0eSBvYmxpZ2F0aw9ucy4wnQYDVR0f
BC4wLDAPoCigJoYKAHR0cDovL2Nybc5zdGFydHNzbc5jb20vY3J0MS1jcmluY3Js
MIG0BggrBgEFBQCBAQSgBTB/MdkGCCsgAQUFBzABhi1odHRwOi8vb2Nzc5zdGFy
dHNzbc5jb20vc3ViL2NsYXNzMS9zZXJ2ZXIvY2EwQGYIKwYBBQUHMAKNmh0dHA6
Ly9haWEuc3RhcnRzc2wuY29tL2NlcHRzL3N1Yi5jbGFzc2Euc2VydmlVylmNhLmNy
dDAjBgNVHRIEHDAahhhodHRwOi8vd3d3LnN0YXJ0c3NsLmNvbS8wDQYJKoZIhvcN
AQELBQADggEBAJE2K2Ofda4eZK7wkL2Qshpa3AQtaR1mBTIOsn5CiDoalfbGH14hf
uNeuqSunchjCqa+HcBxaIoBl18X3iq7ATCoDOM0GRSWePZoxandN4FunAei7A4mf
```



```

tVbzhUV10+VQHwSL5qBaPucAroXQ+/8gA2TLrQLhxpFy+KNN1t7ozD+hiqLjfDen
xk+PNdb01m4Ge90h2c9W/8swIkn+iQTzhewq8ecf6HWQTd35RvdCNPdFWAwRDYSw
xtpdPvkBnuhf2lWVvnQce/xNFE+sfLVHfXv0pQ1JHpXo9xLBzP92piVH0PN1Nb6X
t1gW66pceG/sUzCv6gRNzKkC4/C2BBL2MLERPZB0VmTX3DxDX3M570uvh+v2/miI
RHLq0gfGabDBoYvvF0nXYbFFSF87ICHpw7LM9NfpMFULFWE7epTj69m8f5SuauNi
YpaoZHy4h/OZMn6SoIk+u/hlz8nyMPyLwcKmltdfieFcNID1j0cHL7SRv7Gifl9L
WtBbnySGBVFAaQNLQ0lxXeBvLDRr9hvYqbBMfLPrj0jfyj01SPo2ShpTpjMM0InN
SRXNiTE8kMBY12VLUjWKRhFEuT20KGWmPnmEXAhEKa2wNREuIU640ucQPL2Eg7PD
wuTSxv0JS3QJ3fGz0xk+gA2iCxnw00fFwq/iI9th4p1cbiCJSS4jarJiwUW0n6+L
p/Ei0/h94pDQehn7Skzj0n1fSoMD7SfWI55rjbRZotnvbIip3XUZPD9MEI3vu3Un
0q6Dp6j0W6c=
-----END CERTIFICATE-----
---
Server certificate
subject=/C=UA/CN=demo-srv.webitel.com/emailAddress=chuchko@it-sfera.com.ua
issuer=/C=IL/O=StartCom Ltd./OU=Secure Digital Certificate Signing/CN=StartCom Class 1 Primary Intermediate
Server CA
---
No client certificate CA names sent
---
SSL handshake has read 5113 bytes and written 581 bytes
---
New, TLSv1/SSLv3, Cipher is AES256-GCM-SHA384
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol : TLSv1.2
    Cipher : AES256-GCM-SHA384
    Session-ID: C8F6693AD88FA82ED2DE49B0667BC6E67D88715C5F3A7CE072D76AD29EFB1CB4
    Session-ID-ctx:
    Master-Key: C5D3AACDE2B690ADFF1FC20C529D2E225BDB7AC1381E5AF8A6C65CC7B67319C1F82C3816685E8EE73EDAE8155D72A33E
    Key-Arg : None
    Krb5 Principal: None
    PSK identity: None
    PSK identity hint: None
    TLS session ticket lifetime hint: 300 (seconds)
    TLS session ticket:
0000 - 3f 5a f8 d5 39 eb 0f 1a-d9 79 f0 60 a4 6f 25 13    ?Z..9....y.`.o%.
0010 - 64 d8 ac a9 de 32 af cf-e6 fe e5 05 99 86 46 5a    d....2.....FZ
0020 - e7 68 11 1d 50 d2 89 5f-ab e7 fe 3f ad 31 a9 62    .h..P.._...?.1.b
0030 - 05 b5 4c 46 7e a6 4f c2-b1 e1 24 bd 5b 87 52 73    ..LF~.0...$.[.Rs
0040 - ae 29 e3 dc 89 8a b3 53-32 56 eb 1a 84 8f 7a c9    .).....S2V....z.
0050 - b9 5f ec 93 21 87 48 d7-d3 f3 6a cd 25 9a bb e7    ._.!.H...j.%...
0060 - 0f c2 40 27 ea 28 0c a5-e7 7d 1b c4 ff cf 6c 7e    ..@'...(.)...l~
0070 - 11 db 58 10 8d 5d ee 45-0f 04 29 f2 3f 78 1e 09    ..X..].E..).?x..
0080 - c1 ea e5 bc e7 1b 30 b0-7b 4a 51 c3 3b 9a fe bb    .....0.{JQ.;...
0090 - f4 c9 75 66 62 fe ad 78-8d d0 3d 76 4e 59 6c d4    ..ufb..x..=vNYl.
    Start Time: 1412057396
    Timeout : 300 (sec)
    Verify return code: 0 (ok)
---

```

- [Elasticsearch read-only?](#)
- [bpm'online on-site HTTPS](#)
- [StartSSL wss](#)
- [Chrome Ubuntu Linux](#)
- [http Chrome webrtc](#)