Common Troubleshooting Issues with Certificates in Sonus SBC 1000-2000

In this troubleshooting article, we present various issues, difficulties, and nuances of employing certificates on the Sonus SBC 1000/2000. Each of the instances is accompanied by an investigation path to assist in remedying the issue.

Related Articles

- Working with Sonus SBC 1000/2000 Certificates

Certificate Errors from the Sonus SBC 1000/2000 Log

Certificate Not Trusted

```
[2010-07-01 23:28:47,440] com.net.ux.sip.libctl DEBUG (TransportTlsSocket.cpp:2127) - Verify
peer certificate depth=1, issuer: /DC=net/DC=vx/CN=vx-DEMO5-CA, subject:
/DC=net/DC=vx/CN=vx-DEMO5-CA, status: 0(ok)
[2010-07-01 23:28:47,451] com.net.ux.sip.libctl DEBUG (TransportTlsSocket.cpp:2127) - Verify
peer certificate depth=0, issuer: /DC=net/DC=vx/CN=vx-DEMO5-CA, subject:
/C=US/ST=California/L=Fremont/OU=Sonus SBC 1000/2000/CN=sba1.vx.net, status: 0(ok)
[2010-07-01 23:28:47,453] com.net.ux.sip.libctl DEBUG (TransportTlsSocket.cpp:2025) -
Received peer server certificate common name: sba1.vx.net for conn_id: 1
[2010-07-01 23:28:47,454] com.net.ux.sip.libctl WARN (TransportTlsSocket.cpp:2395) -
Configured host FQDN: sba.net.com does not match peer certificate Common Name: sba1.vx.net
for conn_id: 1
[2010-07-01 23:28:47,455] com.net.ux.sip.libctl WARN (TransportTlsSocket.cpp:2459) -
Configured host FQDN: sba.net.com does not match peer certificate SAN for conn_id: 1
[2010-07-01 23:28:47,459] com.net.ux.sip.libctl WARN (TransportTlsSocket.cpp:2056) - Peer
certificate verify and authentication failed with error: 27(certificate not trusted)
```

Investigation Path:

- Reboot the Sonus SBC 1000/2000.
- The FQDN programmed as a destination SIP Serverdoes not match the Common or Subject Alternative Name within the received certificate.
  - Change the SIP Server configuration to match the FQDN names within the certificate.
- The SIP Server is programmed with the IP instead of the certificate's matching FQDN for the destination host.

Certificate and Private Key Do Not Match

Failed to authenticate (Server) certificate due to bad encoding format, certificate contents or signature mis-match

```
[2011-03-15 13:58:31,910] com.net.ux.csm DEBUG (CertManager.cpp:617) - Received Import
Config Data Approve Request
[2011-03-15 13:58:31,910] com.net.ux.csm TRACE (CertManager.cpp:977) - Approving the
Certificate Contents for File: CertImport20110315135831-000000.pem in holding path
[2011-03-15 13:58:31,912] com.net.ux.csm ERROR (CertManager.cpp:4055) - Unable to load
Server certificate file
[2011-03-15 13:58:31,915] com.net.ux.csm TRACE (CertManager.cpp:3841) - Successfully loaded
Server PKCS7 chain file
[2011-03-15 13:58:31,915] com.net.ux.csm DEBUG (CertManager.cpp:3959) - Writing certificate
chain num: 0
[2011-03-15 13:58:31,916] com.net.ux.csm DEBUG (CertManager.cpp:3959) - Writing certificate
chain num: 1
[2011-03-15 13:58:31,916] com.net.ux.csm DEBUG (CertManager.cpp:3959) - Writing certificate
chain num: 2
[2011-03-15 13:58:31,917] com.net.ux.csm DEBUG (CertManager.cpp:3959) - Writing certificate
chain num: 3
[2011-03-15 13:58:31,919] com.net.ux.csm TRACE (CertManager.cpp:4060) - Successfully loaded
Stack of X509 Certificate
[2011-03-15 13:58:31,959] com.net.ux.csm TRACE (CertManager.cpp:3680) - Certificate to be
imported was successfully validated
[2011-03-15 13:58:31,960] com.net.ux.csm TRACE (CertManager.cpp:4108) - Successfully loaded
Server private key
[2011-03-15 13:58:31,960] com.net.ux.csm ERROR (CertManager.cpp:3754) - Local Certificate
and Private Key do not match, error: 0
[2011-03-15 13:58:31,961] com.net.ux.csm ERROR (CertManager.cpp:662) - Import certificate
validation request failed: host name: 192.168.128.2 status: 3
```

Investigation Path:

- Generate, sign and import a new Sonus SBC 1000-2000 certificate.
- Ensure that the OK on the CSR Generation form is only pressed once before importing the signed certificate.

Connection Refused for Invites or Sonus SBC 1000/2000 does not transmit Options (TG down)

Connection Refused

```
[2011-03-16 15:43:33,471] com.net.ux.sip.libctl INFO (TransportTlsSocket.cpp:92) -
TransportTlsSocket: connect object 0x2ced58 contructor: memory block used count: 1120
[2011-03-16 15:43:33,472] com.net.ux.sip INFO (CallSession.cpp:5040) - {SG(5):132 0x2cfb28
0x2a67d0 [1:0:5:1]} HandleCCSetup: Next hop is mediation.vx.net [10.1.1.7]:5070 CR=0
[2011-03-16 15:43:33,473] com.net.ux.sip INFO (CallSession.cpp:5094) - {SG(5):132 0x2cfb28
0x2a67d0 [1:0:5:1]} HandleCCSetup: Received IE_GENERIC_NAME
[2011-03-16 15:43:33,473] com.net.ux.sip INFO (CallSession.cpp:5129) - {SG(5):132 0x2cfb28
0x2a67d0 [1:0:5:1]} HandleCCSetup: Handling SETUP from "" '5103644064' National pres=0 to
'+15105743571' Unknown.
[2011-03-16 15:43:33,475] com.net.ux.sip INFO (CallSession.cpp:5991) - {SG(5):132 0x2cfb28
0x2a67d0 [1:0:5:1]} ManageLicense: Outbound sent MSG_LM_ACQREL to LM. Acquire
[2011-03-16 15:43:33,480] com.net.ux.sip.libctl ERROR (Socket.cpp:698) -
Socket::HandleFDEvent: EPOLLERR fd=30, handle: 0x2ced5c, iSoError = 111 "Connection
refused", Local Port: 24586, Remote IP:Port(10.1.1.7:5070), fd=30
[2011-03-16 15:43:33,480] com.net.ux.sip INFO (ClientTransaction.cpp:615) -
ProcessSocketError: 2b86f8 ClientTransaction::ProcessSocketError=() called
[2011-03-16 15:43:33,481] com.net.ux.sip.libctl INFO (TransportTlsSocket.cpp:92) -
TransportTlsSocket: connect object 0x2b5128 contructor: memory block used count: 1120
[2011-03-16 15:43:33,482] com.net.ux.sip INFO (CallSession.cpp:4441) - {SG(5):132 0x2cfb28
0x2a67d0 [1:0:5:1]} HandleSocketError: Clean up call due to Socket Error
```

OR

Socket::Close and Deletion for OptionServerSession.cpp

```
2011-06-13 13:51:31,044] com.net.ux.sip DEBUG (OptionsServerSession.cpp:88) -
~OptionsServerSession: 286798 OptionsServerSession::~OptionsServerSession() called
[2011-06-13 13:51:31,044] com.net.ux.sip DEBUG (Session.cpp:175) - ~Session: dtor 286798
id=41
[2011-06-13 13:51:31,044] com.net.ux.sip DEBUG (TransportLayer.cpp:191) - Close:
0TLS1297-5067 0x2863e8 fd=16 force=0.
[2011-06-13 13:51:31,044] com.net.ux.sip.libctl INFO (TransportTlsSocket.cpp:188) - TLS
connection no shutdown deletion for conn_id: 423 on handle: 0x288c50, Local Port: 5067,
Remote IP:Port(10.80.61.61:54999), fd=16, current active sockets: 1
[2011-06-13 13:51:31,045] com.net.ux.sip.libctl INFO (TransportTlsSocket.cpp:242) - Sent
alert close notify in object deletion, server fd=-1, client fd=16 for conn_id: 423
[2011-06-13 13:51:31,047] com.net.ux.sip.libctl INFO (TransportTlsSocket.cpp:334) -
TransportTlsSocket: object 0x288c50 destructor: memory block used count: 570
[2011-06-13 13:51:31,047] com.net.ux.sip.libctl INFO (Socket.cpp:205) - Socket::Close and
Deletion: fd=16
[2011-06-13 13:51:31,047] com.net.ux.sip DEBUG (Session.cpp:71) - ~Dialog: dtor called
2869e0
[2011-06-13 13:51:31,047] com.net.ux.sip DEBUG (TransportLayer.cpp:162) -
~TransportConnection: 0TLS1297-5067 0x2863e8.
[2011-06-13 13:51:31,047] com.net.ux.sip DEBUG (Session.cpp:316) - deleteAllDialogs:
Session:: remaining dialogs : 0
```

Investigation Path:

- Verify configuration and that services are started on the TLS target system.
- Verify Lync topology configuration for IPs and ports
- Reboot the Lync server (full reboot)

Error Opening My Certificate File

```
[2010-06-28 06:47:18,279] com.net.ux.sip.libctl DEBUG (TrustedCertMemStore.cpp:161) - get
memory store cert, len: 0, format: 1, entry: 0
[2010-06-28 06:47:18,281] com.net.ux.sip.libctl FATAL (TransportTlsSocket.cpp:871) - Error
opening My server certificate file, format: 1
[2010-06-28 06:47:18,320] com.net.ux.sip.libctl ERROR (TransportTlsSocket.cpp:389) - TLS
Client Handshake Setup failed for conn_id: 2 on handle: 0x3166e0
[2010-06-28 06:47:18,322] com.net.ux.sip.libctl WARN (TransportTlsSocket.cpp:2698) - TLS
Handshake Failed send alert: -1, recvalert: -1 for conn_id: 2 on handle: 0x3166e0
[2010-06-28 06:47:18,323] com.net.ux.sip.libctl DEBUG (TransportTlsSocket.cpp:2482) - Clean
up with abort flag: 1, persist close flag: 1, state: Client Method State, event: Load Server
Certificate Event for conn_id: 2
[2010-06-28 06:47:18,325] com.net.ux.sip ERROR (TransportLayer.cpp:390) - AbortCB:
Connection aborted 0TLS3-24578 0x312100. Err=2 No such file or directory.
```

Investigation Path:

- Sonus SBC 1000/2000's certificate is missing. Verify a certificate has been imported and is present

Certificate Is Not Yet Valid

```
et.ux.sba INFO (syslogd.cpp:191) - SymComms.GetDomainName: System is part of domain 'vx.net'
[2010-06-28 06:55:54,424] com.net.ux.sip.libctl DEBUG (TransportTlsSocket.cpp:277) -
Received Client TLS handshake message for conn_id: 3 on handle: 0x31d018, sd=25
[2010-06-28 06:55:54,426] com.net.ux.sip.libctl DEBUG (TransportTlsSocket.cpp:1578) -
SSL_connect before: socket fd: 25 for conn_id: 3 in state: SSLv3 read server hello A,
[2010-06-28 06:55:54,438] com.net.ux.sip.libctl DEBUG (TransportTlsSocket.cpp:2127) - Verify
peer certificate depth=1, issuer: /DC=net/DC=vx/CN=vx-DEMO5-CA, subject:
/DC=net/DC=vx/CN=vx-DEMO5-CA, status: 0(ok)
[2010-06-28 06:55:54,448] com.net.ux.sip.libctl WARN (TransportTlsSocket.cpp:2122) - Verify
peer certificate depth=0, issuer: /DC=net/DC=vx/CN=vx-DEMO5-CA, subject:
/C=US/ST=California/L=Fremont/OU=Sonus SBC 1000/2000/CN=sba1.vx.net error: 9(certificate is
not yet valid)
[2010-06-28 06:55:54,450] com.net.ux.sip.libctl WARN (TransportTlsSocket.cpp:2056) - Peer
certificate verify and authentication failed with error: 9(certificate is not yet valid)
```

Investigation Path:

- Verify the Valid From: date and time on the Sonus SBC 1000/2000 certificate is before the current time of the Sonus SBC 1000/2000.
- Set the Sonus SBC 1000/2000 time forward to a time past the Valid From: date/time.

Unable To Get Local Issuer Certificate

```
DEBUG (TransportTlsSocket.cpp:1578) - SSL_connect before: socket fd: 26 for conn_id: 3 in
state: before/connect initialization,
[2010-06-28 01:14:26,570] com.net.ux.sip.libctl DEBUG (TransportTlsSocket.cpp:1583) -
SSL_connect after: socket fd: 26 for conn_id: 3 in state: SSLv3 read server hello A,
[2010-06-28 01:14:26,588] com.net.ux.sip.libctl DEBUG (TransportTlsSocket.cpp:277) -
Received Client TLS handshake message for conn_id: 3 on handle: 0x31d650, sd=26
[2010-06-28 01:14:26,590] com.net.ux.sip.libctl DEBUG (TransportTlsSocket.cpp:1578) -
SSL_connect before: socket fd: 26 for conn_id: 3 in state: SSLv3 read server hello A,
[2010-06-28 01:14:26,595] com.net.ux.sip.libctl WARN (TransportTlsSocket.cpp:2122) - Verify
peer certificate depth=0, issuer: /DC=net/DC=vx/CN=vx-DEMO5-CA, subject:
/C=US/ST=California/L=Fremont/OU=Sonus SBC 1000/2000/CN=sba1.vx.net error: 20(unable to get
local issuer certificate)
[2010-06-28 01:14:26,598] com.net.ux.sip.libctl WARN (TransportTlsSocket.cpp:2056) - Peer
certificate verify and authentication failed with error: 20(unable to get local issuer
certificate)
```

Investigation Path:

- The certificate that signed the peer's certificate is not within Sonus SBC 1000/2000's Trusted (root) store.
  - Delete the current root certificate and import/re-import the root certificate that signed the peer's certificate. See Managing Trusted CA Certificates for further information.
- Reboot the Sonus SBC 1000/2000 and check to see if the problems is resolved.

Configured and Expected host FQDN does not match peer certificate Common Name

```
2011-09-28 11:15:28,272] com.net.ux.sip.libctl INFO (TransportTlsSocket.cpp:2880) -
Configured and Expected host FQDN: ,lync-admin.net.com does not match peer certificate
Common Name: fmt-lyncpool01.net.com for conn_id: 14
```

Investigation Path:

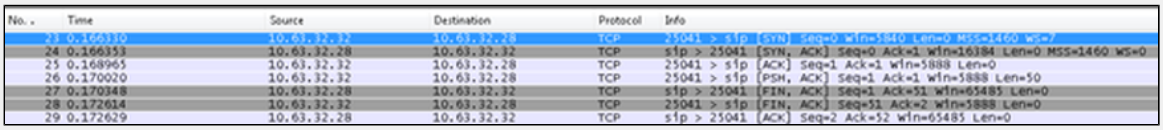
- In the corresponding TLS Profile, set the Validate Client FQDN to Disabled.

Cause
This error occurs when the reverse DNS lookup for the FE returns an FQDN that does not match the Sonus SBC 1000/2000 Federated FQDN configuration. It so happens that in many Lync installations, the FE and the cscp management interface share an IP address, but have two different FQDNs. The reverse lookup, in somes cases, returns the cscp FQDN (which does not match the pool FQDN configured as the Federated FQDN).

SSL Hello Fails

```
1-03-14 17:21:15,251] com.net.ux.sip.libcommon TRACE (AFEventLoop.cpp:92) -
AFEventLoop::Monitor: Adding fd=18 for events=0x1.
[2011-03-14 17:21:15,251] com.net.ux.sip.libctl INFO (TransportTlsSocket.cpp:1926) -
SSL_connect before: socket fd=16 for conn_id: 2 in state: before/connect initialization,
[2011-03-14 17:21:15,252] com.net.ux.sip.libctl INFO (TransportTlsSocket.cpp:1931) -
SSL_connect after: socket fd=16 for conn_id: 2 in state: SSLv3 read server hello A,
[2011-03-14 17:21:15,254] com.net.ux.sip.libctl INFO (Socket.cpp:647) -
Socket::HandleFDEvent: Connection peer shutdown: handle: 0x2556e4, Local Port: 24578, Remote
IP:Port(10.63.32.28:5060), fd=16
[2011-03-14 17:21:15,254] com.net.ux.sip.libctl TRACE (TransportTlsSocket.cpp:2326) -
Received OnSocketClose for conn_id: 2 on handle: 0x2556e0
[2011-03-14 17:21:15,254] com.net.ux.sip.libctl TRACE (TransportTlsSocket.cpp:3047) - TLS
Client clean up with abort flag: 1, persist close flag: 0, state: Handshake State, event:
Socket Close Event for conn_id: 2
[2011-03-14 17:21:15,254] com.net.ux.sip.libctl WARN (TransportTlsSocket.cpp:4450) -
FindTLSConnAlmStEntry: Client Entry Key: (1c203f0a)10.63.32.28 alert code mis-match for
conn_id: 2, Count: 1
[2011-03-14 17:21:15,254] com.net.ux.sip.libctl WARN (TransportTlsSocket.cpp:4475) -
AddTLSConnAlmStEntry: Client Entry=0x2562a0, Key: 1c203f0a was added conn_id: 2 with
AlertSent: -1, AlertRecv: -1, Count: 2
[2011-03-14 17:21:15,255] com.net.ux.sip ERROR (TransportLayer.cpp:581) - AbortCB:
Connection aborted 0TLS3-24578 0x2556e4. Err=11 Resource temporarily unavailable.
[2011-03-14 17:21:15,255] com.net.ux.sip.libctl WARN (TransportTlsSocket.cpp:3350) -
alarmDescStr: TLSv1 Client Handshake failure: conn_id: 2, port: 5060, AlertSent: -1,
AlertRecv: -1. Action: Look up TLS Alert Code definition to fix the problem., len: 147
```

The following is a sniffer trace of the issue:



No.	Time	Source	Destination	Protocol	Info
23	0.166330	10.63.32.32	10.63.32.28	TCP	25041 > sip [SYN] Seq=0 Win=5840 Len=0 MSS=1460 WS=7
24	0.166353	10.63.32.28	10.63.32.32	TCP	sip > 25041 [SYN, ACK] Seq=0 Ack=1 Win=16384 Len=0 MSS=1460 WS=0
25	0.168965	10.63.32.32	10.63.32.28	TCP	25041 > sip [ACK] Seq=1 Ack=1 Win=5888 Len=0
26	0.170020	10.63.32.32	10.63.32.28	TCP	25041 > sip [PSH, ACK] Seq=1 Ack=1 Win=5888 Len=50
27	0.170348	10.63.32.28	10.63.32.32	TCP	sip > 25041 [FIN, ACK] Seq=1 Ack=51 Win=65485 Len=0
28	0.172614	10.63.32.32	10.63.32.28	TCP	25041 > sip [FIN, ACK] Seq=51 Ack=2 Win=5888 Len=0
29	0.172629	10.63.32.28	10.63.32.32	TCP	sip > 25041 [ACK] Seq=2 Ack=52 Win=65485 Len=0

Notice that there is a 50B packet following the TCP handshake and then the other side closes the TCP connection.
The mediation server log indicates a Token failure.

Investigation Path:

- Verify the port numbers are correct in both Sonus SBC 1000/2000 and the target TLS system
- Verify that the FQDNs for the systems are in the DNS server and correct.
- Check the certs and configuration of the peer system. Make sure that the certs are valid and the Sonus SBC 1000/2000 FQDN is configured properly in Exchange or Mediation gateway configurations.

Server Disconnects TLS negotiation

```
[2011-03-15 19:05:32,084] com.net.ux.sip.libctl TRACE (TransportTlsSocket.cpp:1589) - TLS
Client Verify Peer Certificate set for conn_id: 4337
[2011-03-15 19:05:32,085] com.net.ux.sip.libctl TRACE (TransportTlsSocket.cpp:1649) - Set
TLS Server Socket fd=18, sbio: 0x28cd98 for conn_id: 4337
[2011-03-15 19:05:32,085] com.net.ux.sip.libcommon TRACE (AFEventLoop.cpp:92) -
AFEventLoop::Monitor: Adding fd=20 for events=0x1.
[2011-03-15 19:05:32,085] com.net.ux.sip.libctl INFO (TransportTlsSocket.cpp:1926) -
SSL_connect before: socket fd=18 for conn_id: 4337 in state: before/connect initialization,
[2011-03-15 19:05:32,086] com.net.ux.sip.libctl INFO (TransportTlsSocket.cpp:1931) -
SSL_connect after: socket fd=18 for conn_id: 4337 in state: SSLv3 read server hello A,
[2011-03-15 19:05:32,088] com.net.ux.sip.libctl INFO (TransportTlsSocket.cpp:532) - RX
Client TLS handshake message for conn_id: 4337 on handle: 0x269a78, fd=18
[2011-03-15 19:05:32,088] com.net.ux.sip.libctl INFO (TransportTlsSocket.cpp:1926) -
SSL_connect before: socket fd=18 for conn_id: 4337 in state: SSLv3 read server hello A,
[2011-03-15 19:05:32,088] com.net.ux.sip.libctl INFO (TransportTlsSocket.cpp:1931) -
SSL_connect after: socket fd=18 for conn_id: 4337 in state: SSLv3 read server hello A,
[2011-03-15 19:05:32,090] com.net.ux.sip.libctl INFO (TransportTlsSocket.cpp:532) - RX
Client TLS handshake message for conn_id: 4337 on handle: 0x269a78, fd=18
[2011-03-15 19:05:32,090] com.net.ux.sip.libctl INFO (TransportTlsSocket.cpp:1926) -
SSL_connect before: socket fd=18 for conn_id: 4337 in state: SSLv3 read server hello A,
[2011-03-15 19:05:32,099] com.net.ux.sip.libctl TRACE (TransportTlsSocket.cpp:2594) - Verify
peer certificate depth=3, issuer: /C=US/O=GTE Corporation/OU=GTE CyberTrust Solutions,
Inc./CN=GTE CyberTrust Global Root, subject: /C=US/O=GTE Corporation/OU=GTE CyberTrust
Solutions, Inc./CN=GTE CyberTrust Global Root, status: 0(ok)
[2011-03-15 19:05:32,112] com.net.ux.sip.libctl TRACE (TransportTlsSocket.cpp:2594) - Verify
peer certificate depth=2, issuer: /C=US/O=GTE Corporation/OU=GTE CyberTrust Solutions,
Inc./CN=GTE CyberTrust Global Root, subject: /O=Cybertrust, Inc/CN=Cybertrust Global Root,
status: 0(ok)
[2011-03-15 19:05:32,119] com.net.ux.sip.libctl TRACE (TransportTlsSocket.cpp:2594) - Verify
peer certificate depth=1, issuer: /O=Cybertrust, Inc/CN=Cybertrust Global Root, subject:
/O=Cybertrust Inc/CN=Cybertrust SureServer EV CA, status: 0(ok)
[2011-03-15 19:05:32,138] com.net.ux.sip.libctl TRACE (TransportTlsSocket.cpp:2594) - Verify
peer certificate depth=0, issuer: /O=Cybertrust Inc/CN=Cybertrust SureServer EV CA, subject:
/C=US/ST=IL/L=Chicago/streetAddress=161 N Clark
St/1.3.6.1.4.1.311.60.2.1.3=US/1.3.6.1.4.1.311.60.2.1.2=IL/O=Accenture LLP/2.5.4.15=V1.0,
Clause 5.(b)/OU=CIO/serialNumber=00622, status: 0(ok)
[2011-03-15 19:05:32,139] com.net.ux.sip.libctl TRACE (TransportTlsSocket.cpp:2490) - TLS
Client received peer certificate common name: AMROM3205.dir.svc.accenture.com for conn_id:
4337
[2011-03-15 19:05:32,139] com.net.ux.sip.libctl TRACE (TransportTlsSocket.cpp:2874) -
Matched configured host FQDN: amrom3205.dir.svc.accenture.com with peer certificate Common
Name: AMROM3205.dir.svc.accenture.com for conn_id: 4337
[2011-03-15 19:05:32,139] com.net.ux.sip.libctl INFO (TransportTlsSocket.cpp:2532) - TLS
Client peer certificate verified and authenticated for conn_id: 4337
[2011-03-15 19:05:32,233] com.net.ux.sip.libctl INFO (TransportTlsSocket.cpp:1931) -
SSL_connect after: socket fd=18 for conn_id: 4337 in state: SSLv3 read finished A,
[2011-03-15 19:05:32,243] com.net.ux.sip.libctl INFO (Socket.cpp:647) -
Socket::HandleFDEvent: Connection peer shutdown: handle: 0x269a7c, Local Port: 24821, Remote
IP:Port(10.63.32.28:5060), fd=18
[2011-03-15 19:05:32,243] com.net.ux.sip.libctl TRACE (TransportTlsSocket.cpp:2326) -
Received OnSocketClose for conn_id: 4337 on handle: 0x269a78
[2011-03-15 19:05:32,243] com.net.ux.sip.libctl TRACE (TransportTlsSocket.cpp:3047) - TLS
Client clean up with abort flag: 1, persist close flag: 0, state: Handshake State, event:
Socket Close Event for conn_id: 4337
[2011-03-15 19:05:32,243] com.net.ux.sip.libctl WARN (TransportTlsSocket.cpp:4441) -
FindTLSConnAlmStEntry: Client Entry Key: 1c203f0a(10.63.32.28) found for conn_id: 1 with
AlertSent: -1, AlertRecv: -1, Count: 3
[2011-03-15 19:05:32,243] com.net.ux.sip ERROR (TransportLayer.cpp:581) - AbortCB:
Connection aborted 0TLS247-24821 0x269a7c. Err=11 Resource temporarily unavailable.
```

Investigation Path:

- Check the opposing TLS system's logs for indications as to why it closed the session.

Possible incompatible Wave14 Releases (SBA=7306, Sonus SBC 1000/2000=v140/7457)

```
2010-09-09 16:44:20,450] com.net.ux.sip DEBUG (TransportLayer.cpp:408) - ClientConnectedCB:
0TLS10-24585 ssl_id: 9, sd: -1, handle=0x29205c, fd=11, Peer=[172.20.250.133]:5067
[2010-09-09 16:44:20,452] com.net.ux.sip.libctl TRACE (TransportTlsSocket.cpp:1902) - Send
application data_len: 1001 for conn_id: 9 on handle: 0x292058, retry: 0, retry_cnt: 0
[2010-09-09 16:44:20,452] com.net.ux.sip.libctl ERROR (Socket.cpp:590) -
Socket::HandleFDEvent: EPOLLERR fd=11, handle: 0x29205c, iSoError = 32 "Broken pipe", Local
Port: 24585, Remote IP:Port(172.20.250.133:5067), fd=11
[2010-09-09 16:44:20,452] com.net.ux.sip.libctl TRACE (TransportTlsSocket.cpp:2034) -
Received OnSocketClose for conn_id: 9 on handle: 0x292058
[2010-09-09 16:44:20,453] com.net.ux.sip.libctl TRACE (TransportTlsSocket.cpp:2730) - Clean
up with abort flag: 0, persist close flag: 0, state: Application Data State, event: Socket
Close Event for conn_id: 9
[2010-09-09 16:44:20,453] com.net.ux.sip.libctl INFO (TransportTlsSocket.cpp:2776) - TLS
Client connection closed for conn_id: 9 on handle: 0x292058, Local Port: 24585, Remote
IP:Port(172.20.250.133:5067), fd=11, current active sockets: 0
[2010-09-09 16:44:20,454] com.net.ux.sip.libctl TRACE (TransportTlsSocket.cpp:2062) - Tls
Close CBO=0x28cf30 notified to application
[2010-09-09 16:44:20,454] com.net.ux.sip DEBUG (TransportLayer.cpp:507) - CloseCB:
Connection closed 0TLS10-24585 socket=0x29205c connection=0x28cf30.
[2010-09-09 16:44:23,601] com.net.ux.sba WARN (syslogd.cpp:205) -
SymComms.SpawnActionThread: Spawning new thread for action: barSetTime
```

Investigation Path:

- Verify the release level on the Front End server is the same as the SBA release level. All version levels should be 4.0.7577.X

Failure to automatically import the single base64 encoded file containing bundled certificates

The SBC is not able to import base64-encoded bundled certificates. Follow the steps below to import bundled certificates.

- Open the single file provided by the CA vendor as Read-Only.
- Check to see if the file is readable as base64 or PEM encoded format and that it contains bundled certificates.
    - To verify, this file should contain multiple 'Begin Certificate' and 'End Certificate* header lines.
- Copy the first bundled certificate text including the Begin/End header lines
- Paste the first text to *Copy and Paste* option on the Web UI SBC Certificates page(s) based on few criteria listed below.
    - If the bundled file contains the Sonus SBC Certificate, then paste the first text to the Sonus Certificate page via Import X.509 Signed Certificate action and selection of Copy and Paste mode.
    - If the bundled file contains only the Root Chain certificates, then paste the first text to the Trusted CA Certificates page via Import Trusted CA Certificate action and selection of Copy and Paste mode.
- Copy the next bundled certificate text including the Begin/End header lines. Paste the text to the Trusted CA Certificates page.
- Repeat the last step until all the bundled certificates are successfully imported to the Web UI SBC Certificates page(s) one at a time.

Reference

Exchange Log Error: Target name in the certificate is incorrect

> *The Unified Messaging server was unable to exchange the required certificates to enable Transport Layer Security (TLS) with an IP gateway. More information: "A TLS failure occurred because the target name that was specified in the certificate is incorrect. The error code was "1" and the message was "Incorrect function".*

This is caused by some type of FQDN issue on Exchange:

- Ping the Sonus SBC 1000/2000 from Exchange using the Sonus SBC 1000/2000's FQDN
- Verify the Exchange GW configuration is set for FDQN, not IP.
- Reboot the Exchange Server

X509 Certificate Error Messages

An exhaustive list of the error codes and messages is shown below, this also includes the name of the error code as defined in the header file x509_vfy.h Some of the error codes are defined but never returned: these are described as ``unused''.0 X509_V_OK: okthe operation was successful.

2 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT: unable to get issuer certificatethe issuer certificate of a looked up certificate could not be found. This normally means the list of trusted certificates is not complete.
3 X509_V_ERR_UNABLE_TO_GET_CRL: unable to get certificate CRLthe CRL of a certificate could not be found.
4 X509_V_ERR_UNABLE_TO_DECRYPT_CERT_SIGNATURE: unable to decrypt certificate's signaturethe certificate signature could not be decrypted. This means that the actual signature value could not be determined rather than it not matching the expected value, this is only meaningful for RSA keys.
5 X509_V_ERR_UNABLE_TO_DECRYPT_CRL_SIGNATURE: unable to decrypt CRL's signaturethe CRL signature could not be decrypted: this means that the actual signature value could not be determined rather than it not matching the expected value. Unused.
6 X509_V_ERR_UNABLE_TO_DECODE_ISSUER_PUBLIC_KEY: unable to decode issuer public keythe public key in the certificate SubjectPublicKeyInfo could not be read.
7 X509_V_ERR_CERT_SIGNATURE_FAILURE: certificate signature failurethe signature of the certificate is invalid.
8 X509_V_ERR_CRL_SIGNATURE_FAILURE: CRL signature failurethe signature of the certificate is invalid.
9 X509_V_ERR_CERT_NOT_YET_VALID: certificate is not yet validthe certificate is not yet valid: the notBefore date is after the current time.
10 X509_V_ERR_CERT_HAS_EXPIRED: certificate has expiredthe certificate has expired: that is the notAfter date is before the current time.
11 X509_V_ERR_CRL_NOT_YET_VALID: CRL is not yet validthe CRL is not yet valid.
12 X509_V_ERR_CRL_HAS_EXPIRED: CRL has expiredthe CRL has expired.
13 X509_V_ERR_ERROR_IN_CERT_NOT_BEFORE_FIELD: format error in certificate's notBefore fieldthe certificate notBefore field contains an invalid time.
14 X509_V_ERR_ERROR_IN_CERT_NOT_AFTER_FIELD: format error in certificate's notAfter fieldthe certificate notAfter field contains an invalid time.
15 X509_V_ERR_ERROR_IN_CRL_LAST_UPDATE_FIELD: format error in CRL's lastUpdate fieldthe CRL lastUpdate field contains an invalid time.
16 X509_V_ERR_ERROR_IN_CRL_NEXT_UPDATE_FIELD: format error in CRL's nextUpdate fieldthe CRL nextUpdate field contains an invalid time.
17 X509_V_ERR_OUT_OF_MEM: out of memoryan error occurred trying to allocate memory. This should never happen.
18 X509_V_ERR_DEPTH_ZERO_SELF_SIGNED_CERT: self signed certificatethe passed certificate is self signed and the same certificate cannot be found in the list of trusted certificates.
19 X509_V_ERR_SELF_SIGNED_CERT_IN_CHAIN: self signed certificate in certificate chainthe certificate chain could be built up using the untrusted certificates but the root could not be found locally.
20 X509_V_ERR_UNABLE_TO_GET_ISSUER_CERT_LOCALLY: unable to get local issuer certificatethe issuer certificate could not be found: this occurs if the issuer certificate of an untrusted certificate cannot be found.
21 X509_V_ERR_UNABLE_TO_VERIFY_LEAF_SIGNATURE: unable to verify the first certificateno signatures could be verified because the chain contains only one certificate and it is not self signed.
22 X509_V_ERR_CERT_CHAIN_TOO_LONG: certificate chain too longthe certificate chain length is greater than the supplied maximum depth. Unused.
23 X509_V_ERR_CERT_REVOKED: certificate revokedthe certificate has been revoked.
24 X509_V_ERR_INVALID_CA: invalid CA certificatea CA certificate is invalid. Either it is not a CA or its extensions are not consistent with the supplied purpose.
25 X509_V_ERR_PATH_LENGTH_EXCEEDED: path length constraint exceededthe basicConstraints pathlength parameter has been exceeded.
26 X509_V_ERR_INVALID_PURPOSE: unsupported certificate purposethe supplied certificate cannot be used for the specified purpose.
27 X509_V_ERR_CERT_UNTRUSTED: certificate not trustedthe root CA is not marked as trusted for the specified purpose.
28 X509_V_ERR_CERT_REJECTED: certificate rejectedthe root CA is marked to reject the specified purpose.
29 X509_V_ERR_SUBJECT_ISSUER_MISMATCH: subject issuer mismatchthe current candidate issuer certificate was rejected because its subject name did not match the issuer name of the current certificate. Only displayed when the-issuer_checksoption is set.
30 X509_V_ERR_AKID_SKID_MISMATCH: authority and subject key identifier mismatchthe current candidate issuer certificate was rejected because its subject key identifier was present and did not match the authority key identifier current certificate. Only displayed when the-issuer_checksoption is set.
31 X509_V_ERR_AKID_ISSUER_SERIAL_MISMATCH: authority and issuer serial number mismatchthe current candidate issuer certificate was rejected because its issuer name and serial number was present and did not match the authority key identifier of the current certificate. Only displayed when the-issuer_checksoption is set.
32 X509_V_ERR_KEYUSAGE_NO_CERTSIGN:key usage does not include certificate signingthe current candidate issuer certificate was rejected because its keyUsage extension does not permit certificate signing.
50 X509_V_ERR_APPLICATION_VERIFICATION: application verification failurean application specific error. Unused.