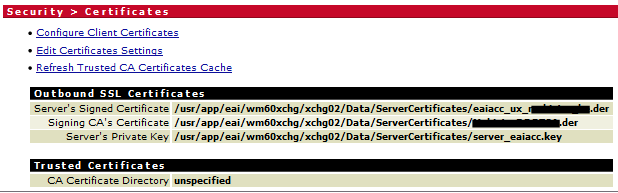
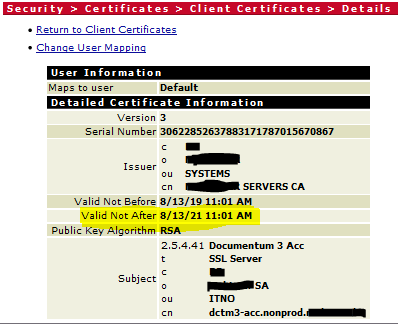
[Some information is censored as they are company confidential, but I hope it won’t hinder your understanding]

Server Certificate configuration:



[Note: watt.security.cert.wmChainVerifier.trustByDefault is set as TRUE for my server; therefore as CA Certificate Directory is “unspecified”, all CA certs will be accepted by wm\_IS]

The certificate from the client I imported:



[Please note: Certificate is valid (highlighted)]

Once I executed the command you suggested I got the below response:

CONNECTED(00000004)

depth=0 name = Documentum 3 Acc, title = SSL Server, C = BE, O = Mobistar SA, OU = ITNO, CN = dctm3-acc.nonprod.mobistar.be

verify error:num=20:unable to get local issuer certificate

verify return:1

depth=0 name = Documentum 3 Acc, title = SSL Server, C = BE, O = Mobistar SA, OU = ITNO, CN = dctm3-acc.nonprod.mobistar.be

verify error:num=21:unable to verify the first certificate

verify return:1

---

Certificate chain

0 s:/name=Documentum 3 Acc/title=SSL Server/C=BE/O=Mobistar SA/OU=ITNO/CN=dctm3-acc.nonprod.mobistar.be

i:/C=BE/O=MOBISTAR/OU=SYSTEMS/CN=MOBISTAR SERVERS CA

-----BEGIN CERTIFICATE-----

#certificate was here but removed by myself#

-----END CERTIFICATE-----

---

Server certificate

subject=/name=Documentum 3 Acc/title=SSL Server/C=BE/O=Mobistar SA/OU=ITNO/CN=dctm3-acc.nonprod.mobistar.be

issuer=/C=BE/O=MOBISTAR/OU=SYSTEMS/CN=MOBISTAR SERVERS CA

---

No client certificate CA names sent

---

SSL handshake has read 2307 bytes and written 463 bytes

---

New, TLSv1/SSLv3, Cipher is DHE-RSA-AES256-GCM-SHA384

Server public key is 2048 bit

Secure Renegotiation IS supported

Compression: NONE

Expansion: NONE

SSL-Session:

Protocol : TLSv1.2

Cipher : DHE-RSA-AES256-GCM-SHA384

Session-ID: E2DBED6838B77607A7E281CD9579A90DEBBFC589F33ADF078BC85BF2B0143956

Session-ID-ctx:

Master-Key: A3C1EB4E2CEA58FB6A441737C58723E421F4A12BF421525A994B851C73671223EF5409D492A394438CF38FC97B637DF9

Key-Arg : None

SRP username: None

TLS session ticket lifetime hint: 300 (seconds)

TLS session ticket:

0000 - 5c fb 78 40 60 49 44 38-3e 23 7a a1 0a ec 11 8a \.x@`ID8>#z.....

0010 - 86 e4 fb d2 97 2c 4c 4d-29 3a 0b 5c 44 1e 62 0a .....,LM):.\D.b.

0020 - 3b 81 80 86 a0 a3 da f4-7d ff 69 49 8d 7f 8d 6b ;.......}.iI...k

0030 - f7 66 54 c1 98 16 bb fa-0f f1 3e 08 95 38 8c 87 .fT.......>..8..

0040 - 93 50 e6 9e a8 64 71 ff-5a a3 03 bf 78 a0 3f a7 .P...dq.Z...x.?.

0050 - a2 78 5a 3d a8 d1 28 ac-a2 d0 6d 2b 2a 19 0a c7 .xZ=..(...m+\*...

0060 - a9 40 b4 1f af 8c 6c 69-b3 19 0e bc 8a 87 74 04 .@....li......t.

0070 - c6 fa 50 51 cd b5 9e 59-57 3e e6 91 05 4b 01 9c ..PQ...YW>...K..

0080 - 9b b3 8c f9 54 47 36 21-42 d6 f5 a2 ad c4 28 17 ....TG6!B.....(.

0090 - f3 38 45 79 4e 18 47 91-66 7b ca ab b3 4d 03 3b .8EyN.G.f{...M.;

00a0 - cb f8 80 ec dc 4f 15 ab-76 50 15 bc b2 48 97 b2 .....O..vP...H..

00b0 - e4 7a b8 02 ca 40 d3 87-87 b9 85 7c d3 2f 5e 55 .z...@.....|./^U

Start Time: 1573620605

Timeout : 300 (sec)

Verify return code: 21 (unable to verify the first certificate)

---

closed