

Question

[Edrian Golob](#) · Mar 9, 2023

ssl3 alert bad certificate or ssl3 alert handshake failure

Hey guys.

I'm having trouble using the Certificate in my BO.

It started to occur after updating the certificate.

I have 2 configurations and 2 certificates, the first one was updated and no error occurs, the second one, the bad certificate or Handshake failure errors occurs. Both have the same configuration.

I already tried marking SSLV3, handshake error occurs. When I unchecked it, a Bad Certificate error occurs.

Do you know what I can do in this case to solve it? I looked for some threads in the community, and I didn't find a solution for my case.

The Certificate works correctly on other systems and platforms.

My Intersystems IRIS version is 2018.1

Errors:

ERROR #6085: Unable to write to socket with SSL/TLS configuration 'GNREPRO', error reported 'SSL/TLS error in SSLconnect(), SSLERRORSSL: protocol error, error:14094412:SSL routines:ssl3_readbytes:ssl3 alert bad certificate'

ERROR #6085: Unable to write to socket with SSL/TLS configuration 'GNREPRO', error reported 'SSL/TLS error in SSLconnect(), SSLERRORSSL: protocol error, error:14077410:SSL routines:SSL23_GET_SERVER_HELLO:ssl3 alert handshake failure'

Nome da Configuração	GNRE_PRO
	Obrigatório.
Descrição	
Habilitado	☒
Tipo	☒ Cliente ☐ Servidor
Seleção de certificado do servidor	☒ Nenhum ☐ Obrigatório
Endereço da Autoridade de Certificação	Procurar...
Estas credenciais do cliente	Obs.: Somente necessário caso este cliente receba pedido para autenticar-se a servidores. Arquivo contendo este certificado de cliente E:\Progress\Certificados\ClienteCert.pem <input <="" div="" type="button" value="Procurar..."/> Arquivo contém chave privada associada E:\Progress\Certificados\privateKey-decrypted.key <input <="" div="" type="button" value="Procurar..."/> Tipo de chave privada ☒ RSA ☐ DSA Senha: ☐ Digitar nova senha ☐ Limpar a senha ☒ Deixar como está
Configurações criptográficas	Protocolos ☐ SSLv3 ☐ TLSv1.0 ☒ TLSv1.1 ☒ TLSv1.2 Ciphersuites habilitadas ALL:!aNULL:!eNULL:!EXP:!SSLv2

log generated by REDEBUG

03/09/23-13:32:46:095 (14200) 0 [Generic.Event] topen for host www.gnre.pe.gov.br device number 49926342
port 443 mode 0x8848 tcpmode 0x24 terminators ibfsz 8192 obfsz 8192 queuesize 5 timeout 5 tcpsbuf=0
tcprbuf=0, XY=off, BINDTO=

03/09/23-13:32:46:095 (14200) 0 [Generic.Event] TCPConnect: SNDBUF sys size=131072, dev size=0

03/09/23-13:32:46:095 (14200) 0 [Generic.Event] TCPConnect: RCVBUF sys size=131072, dev size=0

03/09/23-13:32:46:158 (14200) 0 [Generic.Event]

TCP connected to site 200.238.99.68 port 443

03/09/23-13:32:46:158 (14200) 0 [Generic.Event] StreamInit: SNDBUF sys size=131072, dev size=0

03/09/23-13:32:46:158 (14200) 0 [Generic.Event] StreamInit: RCVBUF sys size=131072, dev size=0

03/09/23-13:32:46:158 (14200) 0 [Generic.Event]

SSL/TLS configuration: GNREPRO

03/09/23-13:32:46:158 (14200) 0 [Generic.Event]

Cipher list: ALL:!aNULL:!eNULL:!EXP:!SSLv2

03/09/23-13:32:46:158 (14200) 0 [Generic.Event]

Certificate file: E:/Progress/Certificados/ClienteCert.pem

03/09/23-13:32:46:158 (14200) 0 [Generic.Event]

Setting private key file encryption password

03/09/23-13:32:46:158 (14200) 0 [Generic.Event]

Private key file: E:/Progress/Certificados/privateKey-decrypted.key

03/09/23-13:32:46:158 (14200) 0 [Generic.Event]

Peer verification option = 0, certificate depth = 9

03/09/23-13:32:46:158 (14200) 0 [Generic.Event]

SSL/TLS client requested.

03/09/23-13:32:46:220 (14200) 0 [Generic.Event]

SSL/TLS error return from SSLconnect().

03/09/23-13:32:46:220 (14200) 0 [Generic.Event]

SSL_ERROR_SSL: protocol error

03/09/23-13:32:46:220 (14200) 0 [Generic.Event]

error:14077410:SSL routines:SSL23GETSERVERHELLO:ssl3 alert handshake failure

03/09/23-13:32:46:220 (14200) 0 [Generic.Event]

[#SOAP](#) [#SSL](#) [#Caché](#)

Product version: Caché 2018.1

Source URL: <https://community.intersystems.com/post/ssl3-alert-bad-certificate-or-ssl3-alert-handshake-failure>