

# Dealing with SSL Exceptions while connecting to TIBCO EMS Over SSL

Every messaging system has its own way of implementing SSL. The best part of DevTest is that the product architecture is extensible and inclusive. An example of the extensibility is its ability to support new versions of J2EE server just with configuration change. In the context of this post, I better talk about the inclusive nature of the product.

The product extensively supports the features of messaging systems. For example, TIBCO EMS supports SSL using various parameters using the JNDI Context. You can add these using the PRO option for Queue connection factory object.

The image shows two overlapping dialog boxes from the Tibco EMS configuration tool. The top dialog, titled 'TibcoSSL', has a 'Name' field set to 'TibcoSSL', an empty 'Description' field, a 'Scope' dropdown set to 'Step', and a 'Class' field set to 'Direct JMS 1.0 Queue Connection Factory for TIBCO EMS'. Below these are 'Properties' for 'Server URL' (ssl://10.74.121.42:7243), 'Default User Name' (admin), and 'Default Password' (empty). A 'Context Properties' section has an 'Open Editor...' button. The bottom dialog, titled 'Context Properties', shows 'SSL Debug Trace' and 'SSL Trace' checked, and 'SSL Enable Verify Host Name' unchecked. A context menu is open over the 'SSL' option, listing various SSL-related settings like 'Security Protocol', 'SSL Auth Only', 'SSL Cipher Suites', etc.

**TibcoSSL** PRO

Name:

Description:

Scope: PRO

Class: Direct JMS 1.0 Queue Connection Factory for TIBCO EMS

**Properties:**

Server URL:

Default User Name:

Default Password:

Context Properties: PRO

**Context Properties**

SSL Debug Trace: PRO ☒

SSL Trace: PRO ☒

SSL Enable Verify Host Name: PRO ☐

Advanced >

SSL >

Add All

- Security Protocol
- SSL Auth Only
- SSL Cipher Suites
- SSL Enable Verify Host
- SSL Expected Host Name
- SSL Host Name Verifier
- SSL Identity
- SSL Identity Encoding
- SSL Password
- SSL Trusted Certificates

Now, let's talk about the various SSL issues one may come across trying to connect to TIBCO EMS Over SSL.

3 / 5

<p>2020-03-27 07:06:30,707 Z (12:36) [SwingWorker-pool-7-thread-1] INFO System. out - SwingWorker-pool-7-thread-1, WRITE: TLSv1 Handshake, length = 118 <b>2020-03-27 07:06:30,758 Z (12:36) [SwingWorker-pool-7-thread-1] INFO System.</b> out - <b>SwingWorker-pool-7-thread-1, READ: TLSv1 Alert, length = 2</b> <b>2020-03-27 07:06:30,759 Z (12:36) [SwingWorker-pool-7-thread-1] INFO System.</b> out - <b>SwingWorker-pool-7-thread-1, RECV TLSv1.2 ALERT: fatal, handshake_failure</b> 2020-03-27 07:06:30,760 Z (12:36) [SwingWorker-pool-7-thread-1] INFO System. out - SwingWorker-pool-7-thread-1, called closeSocket() 2020-03-27 07:06:30,760 Z (12:36) [SwingWorker-pool-7-thread-1] INFO System. out - SwingWorker-pool-7-thread-1, handling exception: <a href="http://java.net/ssl">javax.net.ssl</a>. SSLHandshakeException: Received fatal alert: handshake_failure</p>	<p>The Tibco JMS Client has picked up TLSv1 instead of TLSv1.2.</p>	<p>Check the version of JRE being used. It has been thoroughly validated that TLSv1.2 will be used as default protocol with JRE 1.8. This has been verified with both 10.5 and 10.6</p> <p>See the successful message with TLSv1.2 picked by default.</p> <p>Note that, you dont have to make unnecessary changes to java.security file in order for TLSv1.2 to be picked up. Certain websites suggest to have the following configuration and add TLSV1 to it, but this is unnecessary if you use the JRE that comes with the product.</p> <pre>jdk.tls.disabledAlgorithms=SSLv3, RC4, DES, MD5withRSA, DH keySize &lt; 1024, \ EC keySize &lt; 224, 3DES_EDE_CBC, anon, NULL</pre> <p>trigger seeding of SecureRandom [ 3] done seeding SecureRandom [ 3] Allow unsafe renegotiation: false [ 3] Allow legacy hello messages: true [ 3] Is initial handshake: true [ 3] Is secure renegotiation: false [ 3] Allow unsafe renegotiation: false [ 3] Allow legacy hello messages: true [ 3] Is initial handshake: true [ 3] Is secure renegotiation: false [ 3] %% No cached client session [ 3] update handshake state: client_hello[1] [ 3] upcoming handshake states: server_hello[2] <b>[ 3] *** ClientHello, TLSv1.2</b> [ 3] RandomCookie: GMT: 1569317124 bytes = { 183, 2, 118, 254, 171, 54, 187, 238, 156, 154, 50, 75, 88, 68, 204, 93, 56, 239, 34, 79, 2, 128, 20, 81, 151, 150, 128, 29 } [ 3] Session ID: {} [ 3] Cipher Suites: [TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_DHE_RSA_WITH_AES_256_CBC_SHA256, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_DHE_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_RSA_WITH_AES_256_GCM_SHA384, TLS_DHE_RSA_WITH_AES_256_GCM_SHA384, TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_RSA_WITH_AES_128_GCM_SHA256, TLS_DHE_RSA_WITH_AES_128_GCM_SHA256] [ 3] Compression Methods: { 0 } [ 3] Extension elliptic_curves, curve names: {secp256r1, secp384r1, secp521r1} [ 3] Extension ec_point_formats, formats: [uncompressed] [ 3] Extension signature_algorithms, signature_algorithms: SHA512withECDSA, SHA512withRSA, SHA384withECDSA, SHA384withRSA, SHA256withECDSA, SHA256withRSA, SHA256withDSA, SHA1withECDSA, SHA1withRSA, SHA1withDSA [ 3] Extension extended_master_secret [ 3] Extension renegotiation_info, renegotiated_connection: &lt;empty&gt;</p>
---	---	---

| Message: Error creating queue connection with factory TibcoSSL and username admin: Failed to connect via SSL to [ssl://10.74.121.42:7243]: Failed to connect via SSL to [ssl://10.74.121.42:7243]

| Trapped Exception: Failed to connect via SSL to [ssl://10.74.121.42:7243]: Failed to connect via SSL to [ssl://10.74.121.42:7243]  
| Trapped Message: javax.jms.JMSEException: Failed to connect via SSL to [ssl://10.74.121.42:7243]: Failed to connect via SSL to [ssl://10.74.121.42:7243]

STACK TRACE  
javax.jms.JMSEException:  
Failed to connect via SSL to [ssl://10.74.121.42:7243]: Failed to connect via SSL to [ssl://10.74.121.42:7243]  
at com.tibco.tibjms.TibjmsxLinkSSL.connect (TibjmsxLinkSSL.java:799)

This error typically happens if you dont add the property "SSL Enable Verify Host" even if you don't set a value for this

