IBM MQ C-Based sample amqssslc and
Java GitHub sample SSLSampleJMS.java

https://www.ibm.com/support/pages/node/6983869

Date last updated: 14-Apr-2023

Angel Rivera
IBM MQ Support
https://www.ibm.com/products/mq/support
Find all the support you need for IBM MQ

+++ Question +++

You would like to get more information on how to use MQ API to specify the SSL TLS cipher for an IBM MQ Client application that uses SSL/TLS.

+++ Answer +++

There are 2 samples that provide the details for using the MQ API to specify the SSL TLS cipher:
1: Sample for C-based API applications: amqssslc
2: Sample for JMS: SSLSampleJMS.java

The rest of this note provides more details.

+++ Sample 1: C-base sample to use: amqssslc

The C-based sample amqssslc, shipped with MQ, can be used to test the SSL / TLS connection with the remote queue manager. It uses the API approach to specify the cipher.

Detailed example of using amqssslc:
https://www.ibm.com/support/pages/node/6470619
Using SSL TLS in MQ 9.2 to connect a C-based client in Windows to a queue manager in Linux, using self-signed certificates, 2-way authentication

The sample amqssslc is documented in the manual:

https://www.ibm.com/docs/en/ibm-mq/9.2?topic=multiplatforms-tls-sample-program
IBM MQ / 9.2 /
The TLS sample program
AMQSSSLC is a sample C program that demonstrates how to use the MQCNO and MQSCO structures to supply TLS client connection information on the MQCONNX call. This enables a client MQI application to provide the definition of its client connection channel and TLS settings at run time without a client channel definition table (CCDT).

In Windows, this sample is located at:
  C:\Program Files\IBM\MQ\Tools\c\Samples\Bin64\amqssslc.exe

In Linux, the executable is located at:
        /opt/mqm/samp/bin/amqssslc
The full location of the source sample in Linux is.
        /opt/mqm/samp/amqssslc.c
In Linux, the following MQ fileset needs to be installed:
        MQSeriesSamples
Example of the full name of the fileset for MQ 9.3.2:
        MQSeriesSamples-9.3.2-0.x86_64

Example on how to invoke the sample from Windows:
Notice that the -x is connectionName, and includes both the queue manager and port number, such as:
        -x fortin1.fyre.ibm.com(1419)

Even though the command is shown across several lines, it is a SINGLE long line.
If you copy and paste, ensure that you capture the whole line.

C:\ProgramData\IBM\MQ\ssl>
amqssslc -m QM92TLS -c SSL.SVRCONN -x fortin1.fyre.ibm.com(1419) -k "C:\ProgramData\IBM\MQ\ssl\clientkey" -s TLS_RSA_WITH_AES_128_CBC_SHA256 -l ibmwebspheremqadministrator

+++ Sample 2: JMS sample SSLSampleJMS.java

MQ does not ship a corresponding SSL sample for Java/JMS.
Instead, I found that there is a GitHub Project that has such sample:
    SSLSampleJMS.java

https://github.com/ibm-messaging/mq-tls-ssl-wizard/blob/master/com.ibm.mq.ssl-wizard/src/tlswizard/samples/SSLSampleJMS.java
ibm-messaging / mq-tls-ssl-wizard
.
Disclaimer:
If you have questions about this sample, please use the proper resources under this GitHub project.
That is, the IBM MQ Support Team does not support the samples in this project.

+ begin header from the sample

```
/*********************************************************************/
/*                                                                   */
/* Program name: SSLSampleJMS                                        */
/*                                                                   */
/* Description: Sample JMS program that demonstrates how to          */
/*              specify SSL client connection information for a      */
/*              MQQueueConnectionFactory connection.                 */
/*                                                                   */
/* <START_COPYRIGHT>                                                 */
/* Licensed Materials - Property of IBM                             */
/*                                                                   */
/* (C) Copyright IBM Corp. 2006, 2009 All Rights Reserved.          */
/*                                                                   */
/* US Government Users Restricted Rights - Use, duplication or      */
/* disclosure restricted by GSA ADP Schedule Contract with          */
/* IBM Corp.                                                         */
/* <END_COPYRIGHT>                                                   */
/*                                                                   */
/*********************************************************************/
/*                                                                   */
/* Overview:                                                         */
/*                                                                   */
/*   This sample is provided with WebSphere MQ SupportPac MO04 -     */
/*   WebSphere MQ SSL Wizard. The wizard will generate command line */
/*   options to be used with this program.                          */
/*                                                                   */
/*   It is assumed that the SSL server connection channel and other */
/*   SSL administration, as instructed by the wizard, has been      */
/*   completed before running this program.                         */
/*                                                                   */
/*   If the SSL connection is successful the program should output: */
/*                                                                   */
/*      "Connection Successful!"                                     */
/*                                                                   */
/*********************************************************************/
/*                                                                   */
```

```
/* Function:                                                        */
/*                                                                  */
/*    SSLSampleJMS is a sample Java program that demonstrates how to */
/*    supply SSL information for a client connection on a           */
/*    MQQueueConnectionFactory connection.                          */
/*                                                                  */
/*    The sample simply connects to the queue manager.              */
/*                                                                  */
/********************************************************************/
/*                                                                  */
/* Usage:                                                           */
/*                                                                  */
/*    SSLSampleJMS has 7 parameters, all of which are mandatory:    */
/*                                                                  */
/*      java SSLSampleJMS Conname Port SvrconnChannelName           */
/*              QMgrName SSLCiph SSLKeyr SSLKeyrPassword             */
/*                                                                  */
/*    The parameters are:                                           */
/*                                                                  */
/*      Conname      - the connection name of the server queue      */
/*                     manager in the same format as the CONNAME    */
/*                     parameter on the MQSC DEFINE CHANNEL command, */
/*                     but without the port specified.              */
/*                                                                  */
/*      Port         - the connection port of the server queue      */
/*                     manager.                                      */
/*                                                                  */
/*      SvrconnChannelName                                          */
/*                   - the name of the server connection channel    */
/*                     on the server queue manager with which the   */
/*                     sample program will try to connect.          */
/*                                                                  */
/*      QMgrName     - the name of the server queue manager.        */
/*                                                                  */
/*      SSLCiph      - the SSL CipherSpec.                          */
/*                                                                  */
/*      SSLKeyr      - the name of a single store, which is both the */
/*                     keystore and truststore.                     */
/*                                                                  */
/*      SSLKeyrPassword                                             */
/*                   - the SSL key repository password.             */
/*                                                                  */
/*    For example:                                                  */
/*                                                                  */
/*      java SSLSampleJMS myhost1 1414 SSL.SVRCONN QM1              */
/*                        NULL_MD5 C:\mq\ssl\client.kdb password */
/*                                                                  */
/********************************************************************/
```

+ end header from the sample

+++ end +++