

---

# IBM WebSphere MQ: Integration Guide

---

THALES LUNA HSM

## Document Information

<b>Document Part Number</b>	007-011561-001
<b>Revision</b>	G
<b>Release Date</b>	7 December 2022

## Trademarks, Copyrights, and Third-Party Software

Copyright © 2022 Thales Group. All rights reserved. Thales and the Thales logo are trademarks and service marks of Thales Group and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

# CONTENTS

Overview .....	4
About IBM WebSphere MQ .....	4
Certified Platforms .....	4
Prerequisites .....	5
Configure Luna HSM Device .....	5
Set up IBM WebSphere MQ .....	6
Integrating Luna HSM with IBM WebSphere MQ.....	7
Configure SSL/TLS for IBM WebSphere MQ using Luna HSM.....	7
Create Queue Manager .....	7
Create TLS certificates for MQ Server and MQ Client using Luna HSM .....	8
Configure Queue Manager SSL/TLS to use Luna HSM Keys .....	14
Configure MQ Client for SSL/TLS to use Luna HSM Keys.....	18
Configuring SSL/TLS for IBM WebSphere MQ using Luna HSM .....	19
Contacting Customer Support.....	21
Customer Support Portal .....	21
Telephone Support.....	21

## Overview

This guide is intended to provide instructions for setting up a small test lab that has IBM WebSphere MQ running with Luna HSM to secure the SSL private keys, public keys, and certificates. The guide explains installation and configuration of Luna Client software with IBM WebSphere MQ for storing SSL keys and certificates on Luna HSM.

The integration between Luna HSM and IBM WebSphere MQ uses the IBM Java interface to generate the keys and certificates on Luna HSM. Integration of IBM WebSphere MQ with Luna HSM generates SSL keys. Luna HSM provides security by protecting the private keys within a FIPS 140-2 certified hardware security module.

The benefits of using Luna HSM to generate the SSL keys for IBM WebSphere MQ include the following:

- > Secure generation, storage, and protection of the SSL keys on FIPS 140-2 level 3 validated hardware.
- > Full life cycle management of the keys.
- > HSM audit trail.
- > Significant performance improvements by off-loading cryptographic operations from servers.

## About IBM WebSphere MQ

IBM WebSphere MQ supports the exchange of information between applications, systems, services and files by sending and receiving message data via messaging queues. This simplifies the creation and maintenance of business applications. Secure communications that use the TLS cryptographic security protocols involve setting up the communication channels and managing the digital certificates that you will use for authentication.

IBM WebSphere MQ is a family of network software products launched by IBM in March 1992. It was previously known as MQ Series. It allows independent and potentially non-concurrent applications on a distributed system to communicate with each other.

Luna HSMs provides key management security for certificates and certificate-based authentication, including import of trusted CA certificates from software based keystore to hardware based keystore, and generation of self-signed certificates and personal certificate requests via the IBM Key Management Utility.

## Certified Platforms

This integration is certified on the following platforms.

HSM Type	Platforms Tested	IBM WebSphere MQ
Luna HSM	RHEL	IBM WebSphere MQ v9.1.0.12
Luna HSM	Windows Server	IBM WebSphere MQ v9.1.0.2 with IT15253 (Patch 9.1.0.2-IBM-MQ-Win64-TF55486)

The Patch 9.1.0.2-IBM-MQ-Win64-TF55486 fixes the HSM Password issue “[AMQ9671E: The PKCS #11 token password specified is invalid.](#)” in MQ Client when it communicates to HSM using password provided in MQClient.ini file. The APAR for this fix is IT30722 which can be downloaded from IBM ecurep on request.

**NOTE:** The above patch is not required for IBM MQ v9.1.0.6 or above. If you are using older versions (7.x or 8.x) of IBM WebSphere MQ, please refer the earlier Luna HSM integration guide “[IBM WebSphere MQ Integration Guide RevE](#)”

**Luna HSM:** Luna HSM appliances are purposefully designed to provide a balance of security, high performance, and usability that makes them an ideal choice for enterprise, financial, and government organizations. Luna HSMs physically and logically secure cryptographic keys and accelerate cryptographic processing. The Luna HSM on premise offerings include the Luna Network HSM, Luna PCIe HSM, and Luna USB HSMs. Luna HSMs are also available for access as an offering from cloud service providers such as IBM cloud HSM and AWS cloud HSM classic

## Prerequisites

Before you proceed with the integration, complete the following tasks:

### Configure Luna HSM Device

To configure a Luna HSM device:

1. Ensure that the HSM is set up, initialized, provisioned, and ready for deployment. Refer to the HSM product documentation for help.
2. Create a partition that will be later used for generating SSL keys for IBM MQ.
3. Create and exchange certificate between the Luna Network HSM and Client system. Register client and assign partition to create an NTLS connection. Initialize Crypto Officer and Crypto User roles for the registered partition.
4. Ensure that the partition is successfully registered and configured. The command to see the registered partitions is:

```
C:\Program Files\SafeNet\LunaClient>lunacm.exe
lunacm.exe (64-bit) v10.4.0-417. Copyright (c) 2021 SafeNet. All rights reserved.
```

```
Available HSMs:
Slot Id ->          0
Label ->           TPA01
Serial Number ->   1312109862201
Model ->           LunaSA 7.7.1
Firmware Version -> 7.7.1
Bootloader Version -> 1.1.2
Configuration ->   Luna User Partition With SO (PW) Key Export
                   With Cloning Mode
Slot Description -> Net Token Slot
```

```
FM HW Status ->          Non-FM
Current Slot Id: 0
```

- For PED-authenticated HSM, enable partition policies 22 and 23 to allow activation and auto-activation.

**NOTE:** Refer to [Luna HSM documentation](#) for detailed steps on creating NTLS connection, initializing the partitions, and assigning various user roles.

## Set up Luna HSM in FIPS Mode

**NOTE:** This setting is not required for Luna HSM Universal Client. This setting is applicable only for Luna HSM Client 7.x.

Under FIPS 186-3/4, the RSA methods permitted for generating keys are 186-3 with primes and 186-3 with aux primes. This means that RSA PKCS and X9.31 key generation is no longer approved for operation in a FIPS-compliant HSM. If you are using Luna HSM in FIPS mode, you have to make the following change in the configuration file:

```
Misc = {
RSAKeyGenMechRemap = 1;
}
```

The above setting redirects the older calling mechanism to a new approved mechanism when Luna HSM is in FIPS mode.

**NOTE:** If IBM MQ is using CKM\_SHA1\_RSA\_PKCS mechanism for signing the data with Luna SA f/w 7.x.x, upgrade the firmware to 7.7.0 or above to use CKM\_SHA256\_RSA\_PKCS mechanism which is supported in FIPS mode.

## Configure Luna HSM HA (High-Availability)

Please refer to [Luna HSM documentation](#) for HA steps and details regarding configuring and setting up two or more HSM appliances on Windows and UNIX systems. You must enable the HAOnly setting in HA for failover to work so that if primary stop functioning for some reason, all calls automatically routed to secondary till primary starts functioning again.

**NOTE:** This integration is tested in both HA and FIPS mode.

## Set up IBM WebSphere MQ

IBM WebSphere MQ (Server or Client) must be installed on the target machines to carry on with the integration process. You can install IBM WebSphere MQ explorer for a Windows or Linux system. This graphical tool enables you to explore and configure all WebSphere MQ objects and resources and can remotely connect to queue managers on any supported platform. You also need to create the required user ID and group ID before you install WebSphere MQ. For a detailed installation procedure, refer to the IBM WebSphere MQ documentation.

<https://www.ibm.com/docs/en/ibm-mq>

## Integrating Luna HSM with IBM WebSphere MQ

Luna HSM provides strong physical protection of secure assets, including keys, and should be considered a best practice when using IBM MQ. Following are the steps involved in this integration:

- > [Configuring SSL/TLS for IBM WebSphere MQ using Luna HSM](#)
- > [Verifying SSL/TLS connectivity between MQ Server and MQ Client](#)

### Configure SSL/TLS for IBM WebSphere MQ using Luna HSM

To set up your SSL/TLS installation, you must start the queue manager, obtain and manage your digital certificates, and configure TLS to use Luna HSM.

**NOTE:** On a test system, you can use self-signed certificates or certificates issued by a local certificate authority (CA). On a production system, use certificates issued by a trusted CA.

Following are the steps to configure IBM WebSphere MQ with Luna HSM:

- > [Create Queue Manager](#)
- > [Create TLS certificates for MQ Server and MQ Client using Luna HSM](#)
- > [Configure Queue Manager SSL/TLS to use Luna HSM Keys](#)
- > [Configure MQ Client for SSL/TLS to use Luna HSM Keys](#)

### Create Queue Manager

Before you can use messages and queues, you must create and start at least one queue manager and its associated objects. To create and start the Queue Manager:

1. Log on to the IBM MQ Server as Administrator or a user added in mqm group and create a queue manager, if not created already.
2. To create the queue manager, open the command prompt from the <IBM MQ Installation Directory>/bin folder and then run the following command:

**Windows:**

```
C:\Program Files\IBM\MQ\bin>crtmqm.exe QM1
```

**Linux:**

```
$ /opt/mqm/bin/crtmqm QM1
```

Where **QM1** is queue manager name.

3. After creating the queue manager, start the queue manager using the following command:

**Windows:**

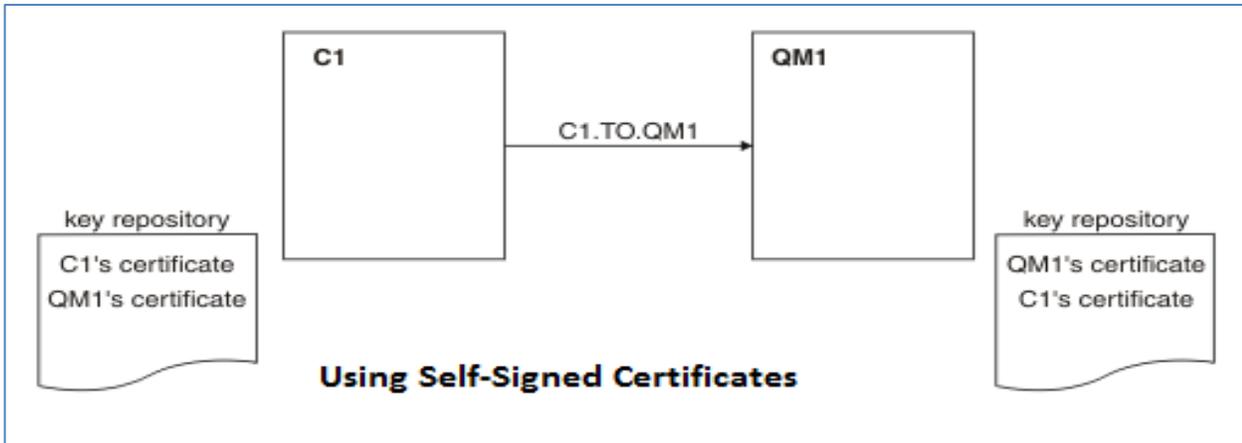
```
C:\Program Files\IBM\MQ\bin>strmqm.exe QM1
```

**Linux:**

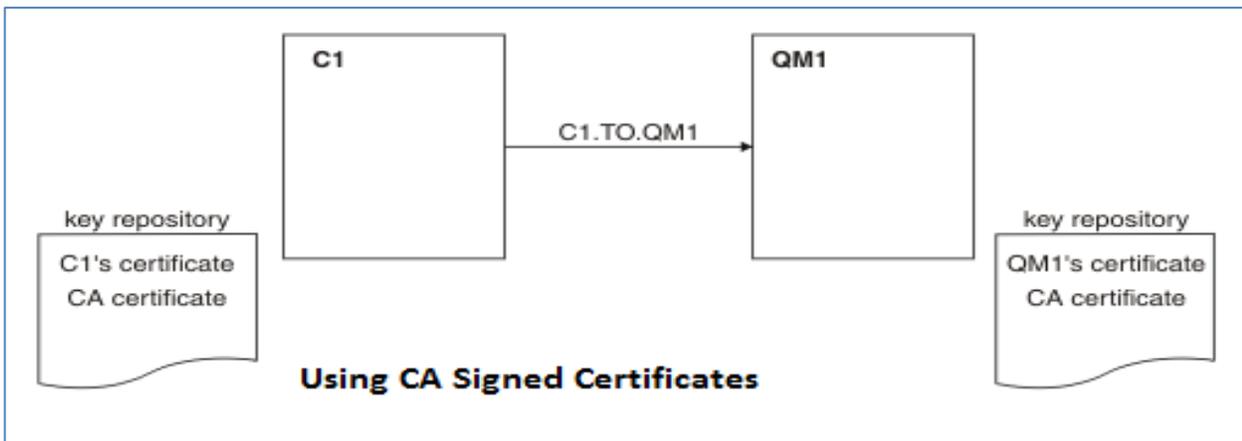
```
$ /opt/mqm/bin/strmqm QM1
```

## Create TLS certificates for MQ Server and MQ Client using Luna HSM

You can use a self-signed certificate or CA signed certificate as per your requirement. The steps provided here depict how to use a self-signed certificate. To use a CA signed certificate, you need to obtain the CA signed certificate and import both the CA certificate and the signed certificate into the key database.



In the above figure, the key repository for QM1 contains the certificate for QM1 and the public certificate from C1. The key repository for C1 contains the certificate for C1 and the public certificate from QM1.



In the above figure, the key repository for C1 contains certificate for C1 and the CA certificate. The key repository for QM1 contains the certificate for QM1 and the CA certificate.

To create the SSL/TLS certificate/key on Luna HSM:

**NOTE:** These steps require to be executed on both MQ Server and MQ Client if you are securing both MQ Server and MQ Client SSL keys on Luna HSM.

1. Log on to the IBM MQ Server using the Administrator account or user added in the MQM group.
2. Create the luna.cfg file with the following contents and save the file at any location.

**NOTE:** Path to Linux library = /usr/safenet/lunaclient/lib/libCryptoki2\_64.so.

```

name = LUNA
library = C:\Program Files\SafeNet\LunaClient\cryptoki.dll
description = Luna config
slotListIndex = 0
attributes (*, CKO_PRIVATE_KEY, *) = {
CKA_SENSITIVE = true
CKA_SIGN=true
CKA_DECRYPT=true
}
attributes (*, CKO_PUBLIC_KEY, *) = {
CKA_VERIFY=true
CKA_ENCRYPT=true
}
attributes (*, CKO_SECRET_KEY, *) = {
CKA_SENSITIVE = true
CKA_ENCRYPT=true
CKA_DECRYPT=true
CKA_SIGN=true
CKA_VERIFY=true
}
disabledMechanisms = {
CKM_SHA1_RSA_PKCS
}

```

3. Open <IBM MQ installation directory>\java\jre\lib\security\java.security file and edit IBMPKCS11 provider with the path to luna.cfg as follows:

**NOTE:** Replace <Path to luna.cfg file> with actual path of luna.cfg file.

```

security.provider.1=com.ibm.fips.jsse.IBMJSSEFIPSPProvider
security.provider.2=com.ibm.crypto.fips.provider.IBMJCEFIPS
security.provider.3=com.ibm.jsse2.IBMJSSEProvider2
security.provider.4=com.ibm.crypto.provider.IBMJCE
security.provider.5=com.ibm.security.jgss.IBMJGSSProvider
security.provider.6=com.ibm.security.cert.IBMCertPath

```

```

security.provider.7=com.ibm.crypto.pkcs11impl.provider.IBMPKCS11Impl
<Path to luna.cfg file>
security.provider.8=com.ibm.security.sasl.IBMSASL
security.provider.9=com.ibm.xml.crypto.IBMXMLCryptoProvider
security.provider.10=com.ibm.xml.enc.IBMXMLEncProvider
security.provider.11=com.ibm.security.jgss.mech.spnego.IBMSPNEGO
security.provider.12=sun.security.provider.Sun
security.provider.13=com.ibm.security.cmskeystore.CMSProvider

```

- Run the strmqikm.exe from the <IBM MQ installation directory>/bin directory.

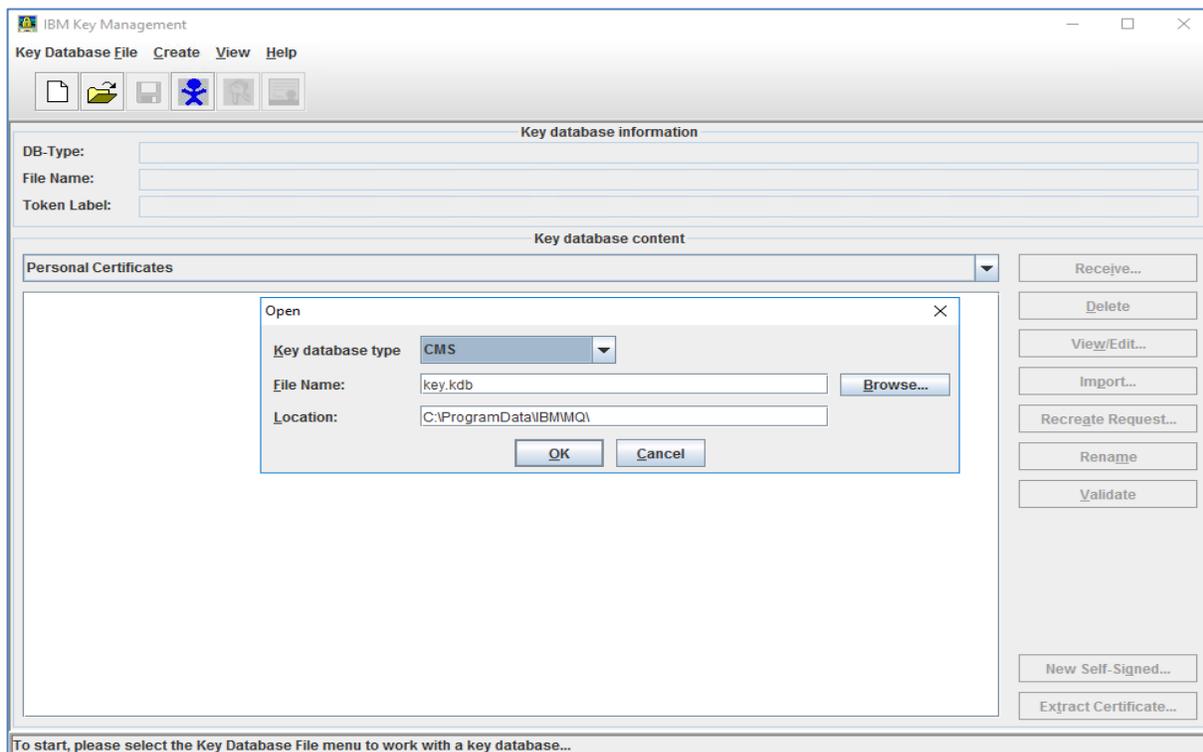
#### **Windows:**

```
C:\Program Files\IBM\MQ\bin>strmqikm.exe
```

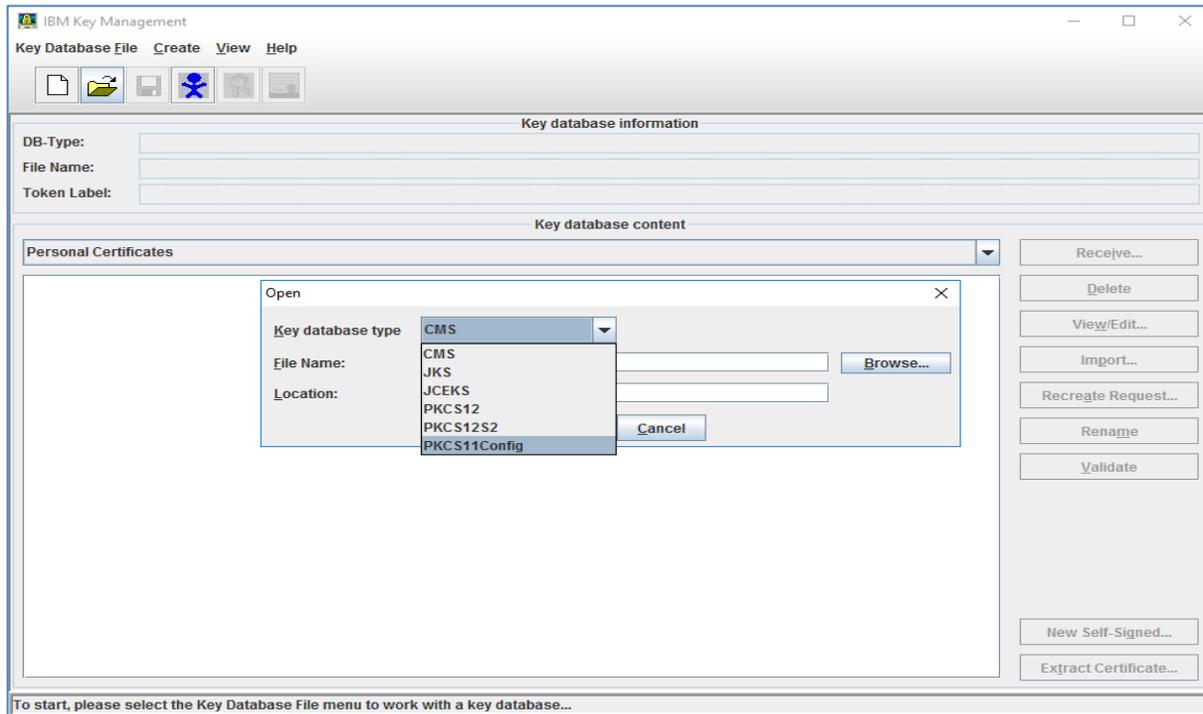
#### **Linux:**

```
$ /opt/mqm/bin/strmqikm
```

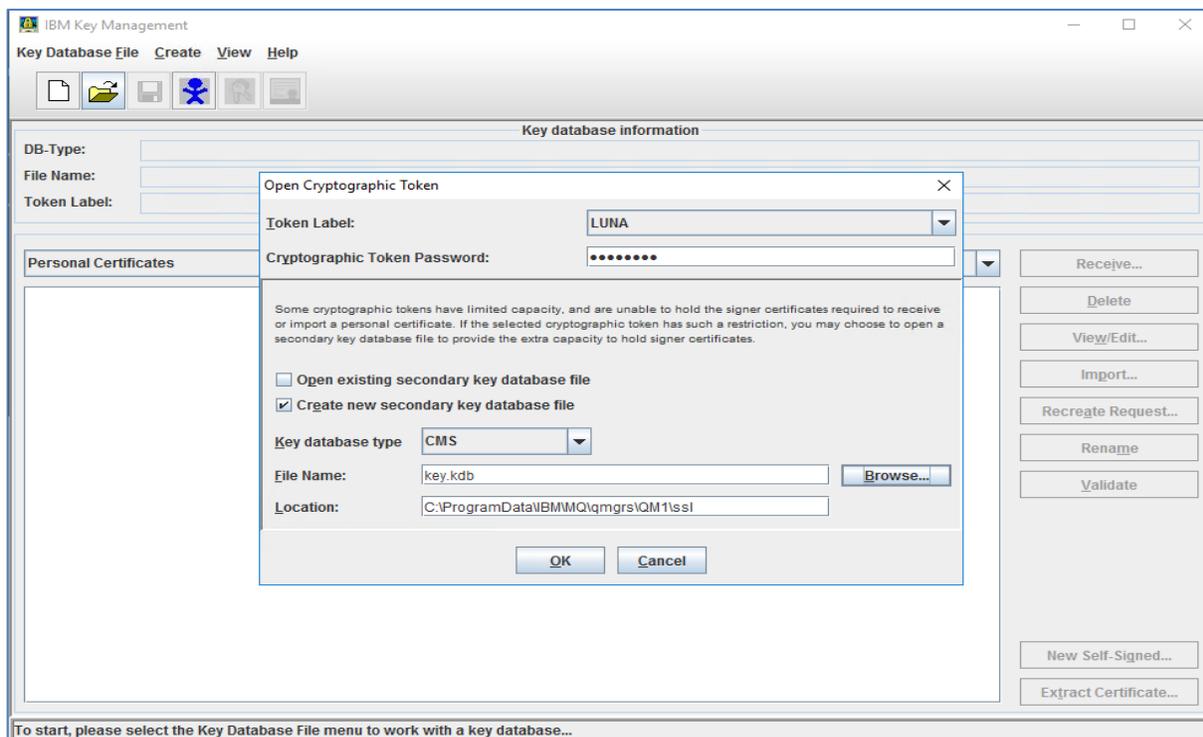
- When IBM Key Management windows pops up, click **Key Database File > Open**.



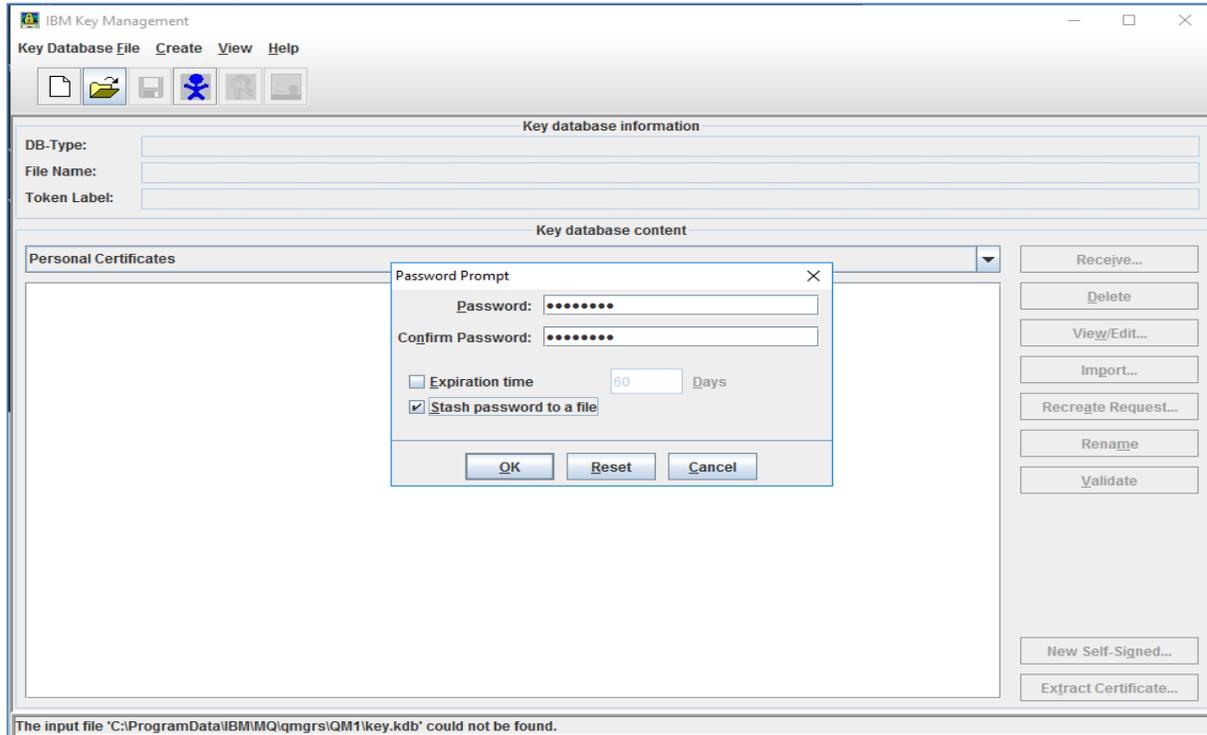
6. Select **PKCS11Config** from Key database type drop-down and click **OK**.



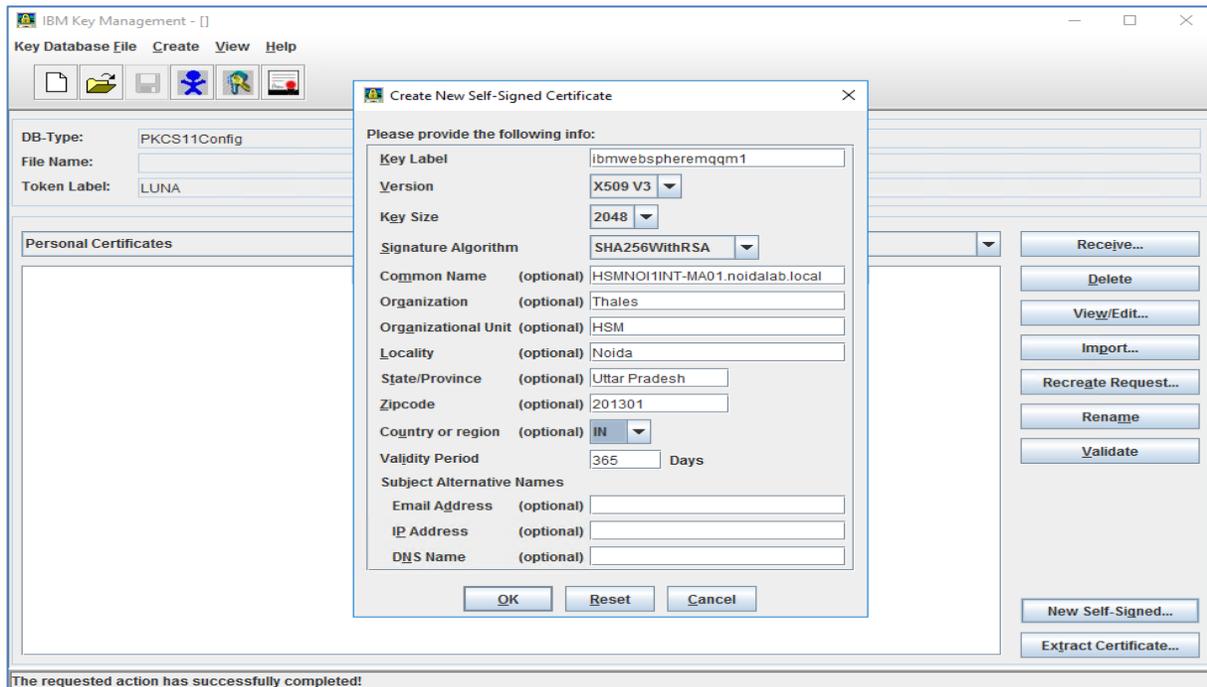
7. Enter partition password in **Cryptographic Token Password**, select **Create new secondary key database file**, and then click **Browse...** to select the key.kdb file location. Click **OK** after selecting the file location.



8. A password prompt window will pop up. Create a password for key.kdb file, select the **Stash password to a file** checkbox, and then click **OK**.

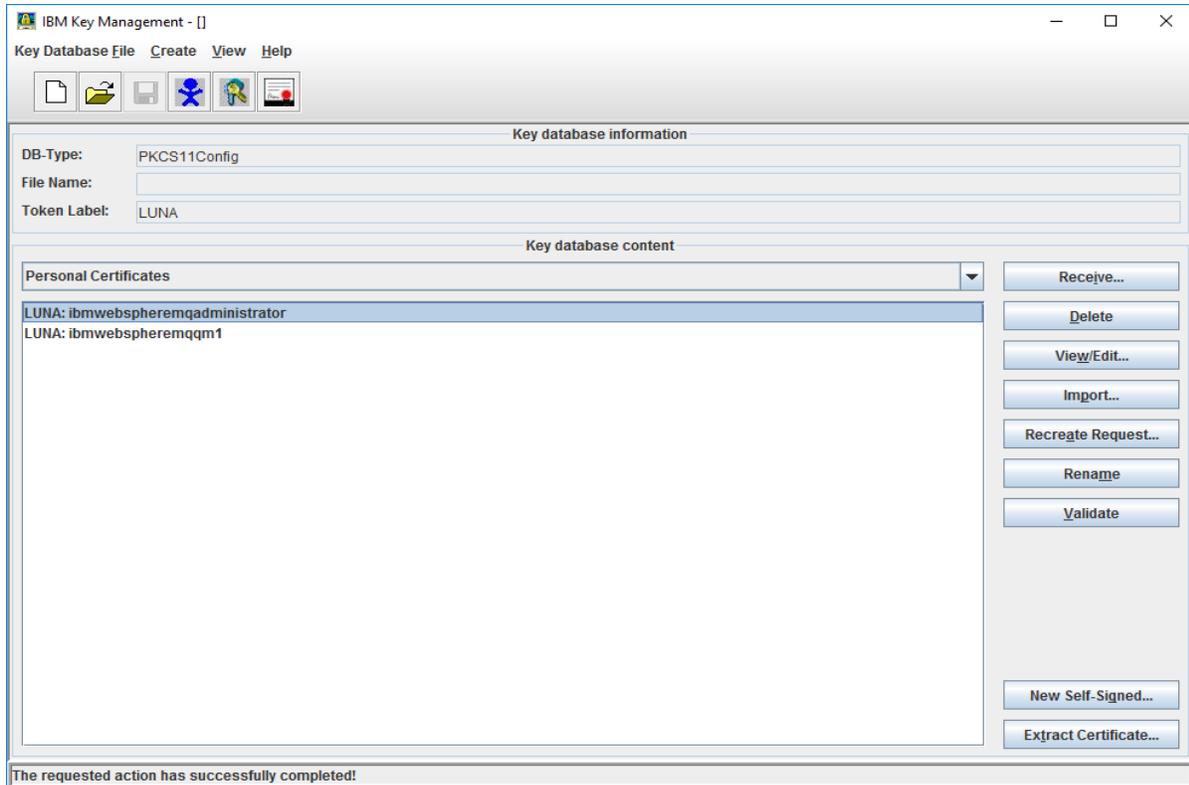


9. Click **Create - New Self-Signed Certificate**. Enter the Key Label in lowercase letters in the specific format “ibmwebspheremq+queuename”, where queuename is the name of the queue manager. Enter all other details for the certificate and then click **OK**.



10. Log on to the IBM MQ Client using the administrator or user account added in the MQM group.

11. Repeat steps 1-9 for MQ Client to generate the IBM MQ Client certificate, while ensuring that IBM MQ Client Key Label also has the specific format “ibmwebspheremq+<logged\_in\_user>” with lowercase letters. Both MQ Server and Client Certificates are generated on the SafeNet Luna HSM partition and are visible under Personal Certificates.



**NOTE:** For demonstration purpose in this guide, the same partition and self-signed certificate is used for both MQ Server and Client, but it is recommended to use separate partition and CA signed certificates for MQ Server and Client.

12. Export the Server Certificate. To export the MQ Server certificate, select the certificate **under Personal Certificate** and click **Extract Certificate....** Then, save the certificate file and transfer the file to the MQ Client.
13. To import the Server Certificate on MQ Client, select **Signer Certificate** from Key database content drop-down and click **Add....** Then, browse the server certificate you transferred, and click **OK** to add the Server certificate. Next, provide a label for the certificate and click **OK**.

Repeat steps 12-13 to export the Client certificate and add it to the Server certificate database.

**NOTE:** If you are using a CA signed certificate, you are required to add the CA public certificate of MQ Server in certificate database of MQ Client and vice-versa.

## Configure Queue Manager SSL/TLS to use Luna HSM Keys

IBM MQ Server must be configured to use the Luna HSM for certificate and keys used to create the SSL/TLS connection with client. To configure the IBM MQ Server:

1. Log on to the IBM MQ Server using Administrator or user added in the mqm group.
2. Run the MQExplorer.exe from the <IBM MQ installation directory>/bin directory.

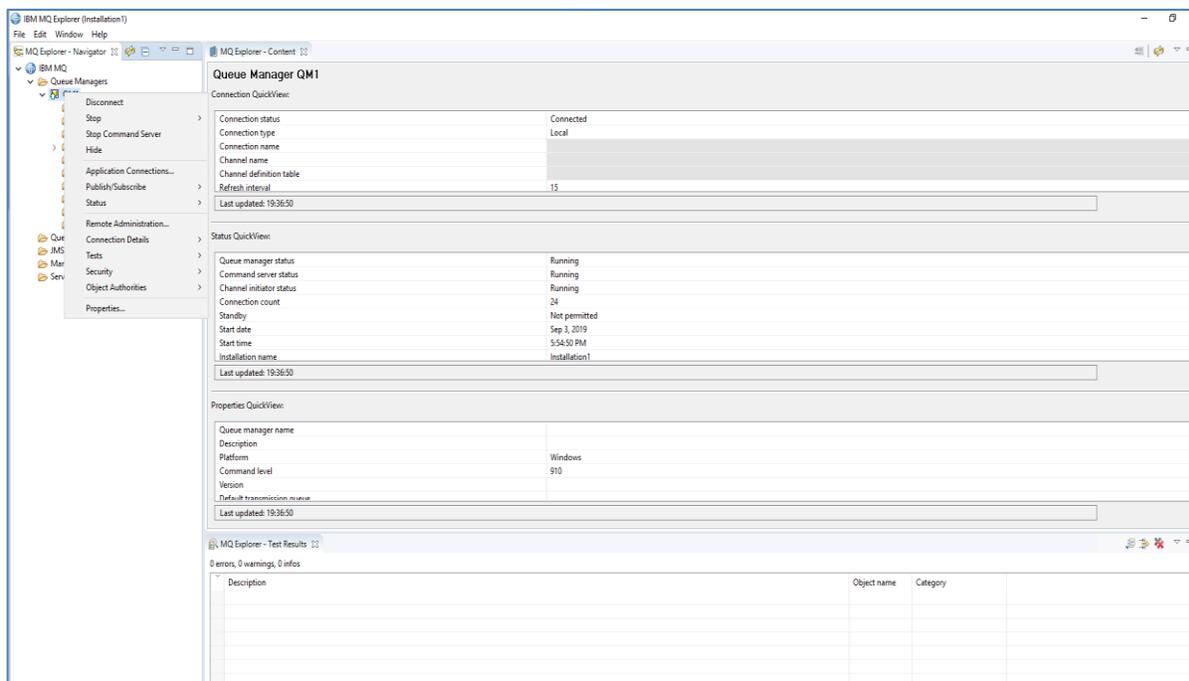
### **Windows:**

```
C:\Program Files\IBM\MQ\bin>MQExplorer.exe
```

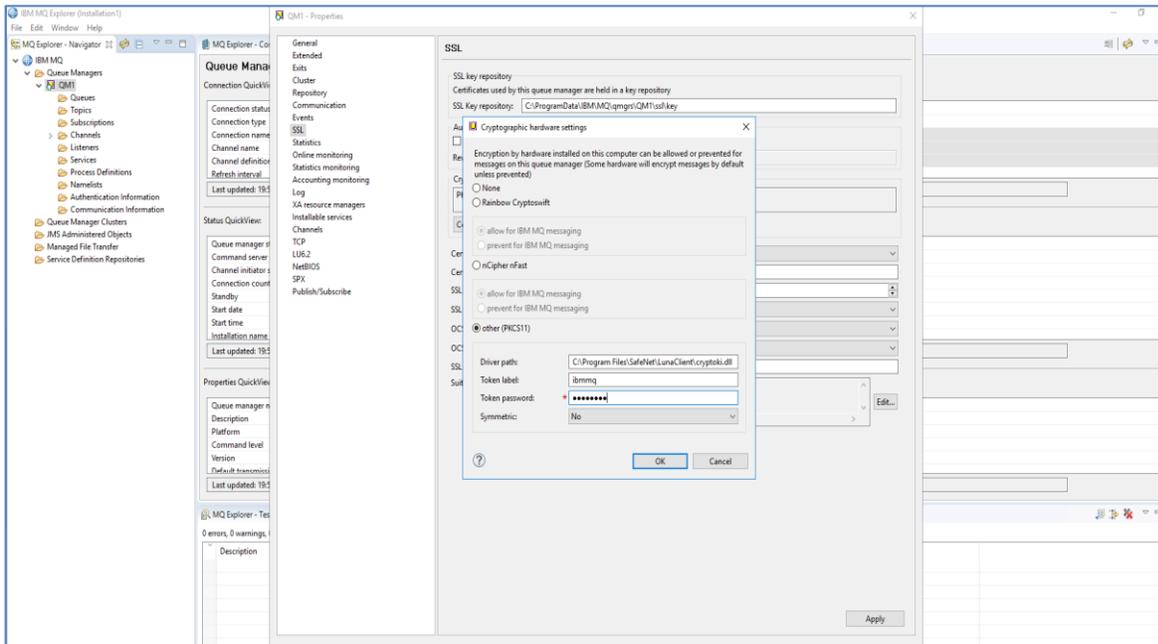
### **Linux:**

```
$ /opt/mqm/bin/MQExplorer
```

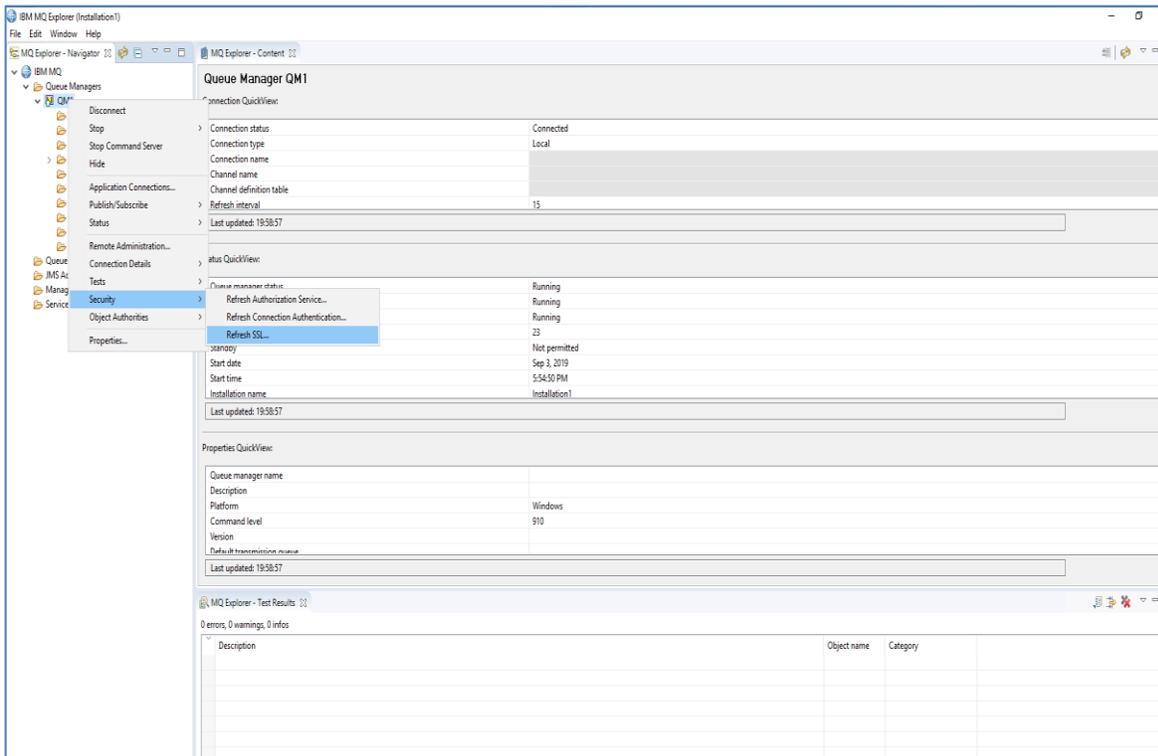
3. In **MQ Explorer–Navigator** pane, expand **IBM MQ > Queue Managers**, right-click on queue manager you have created, and then click **Properties....**



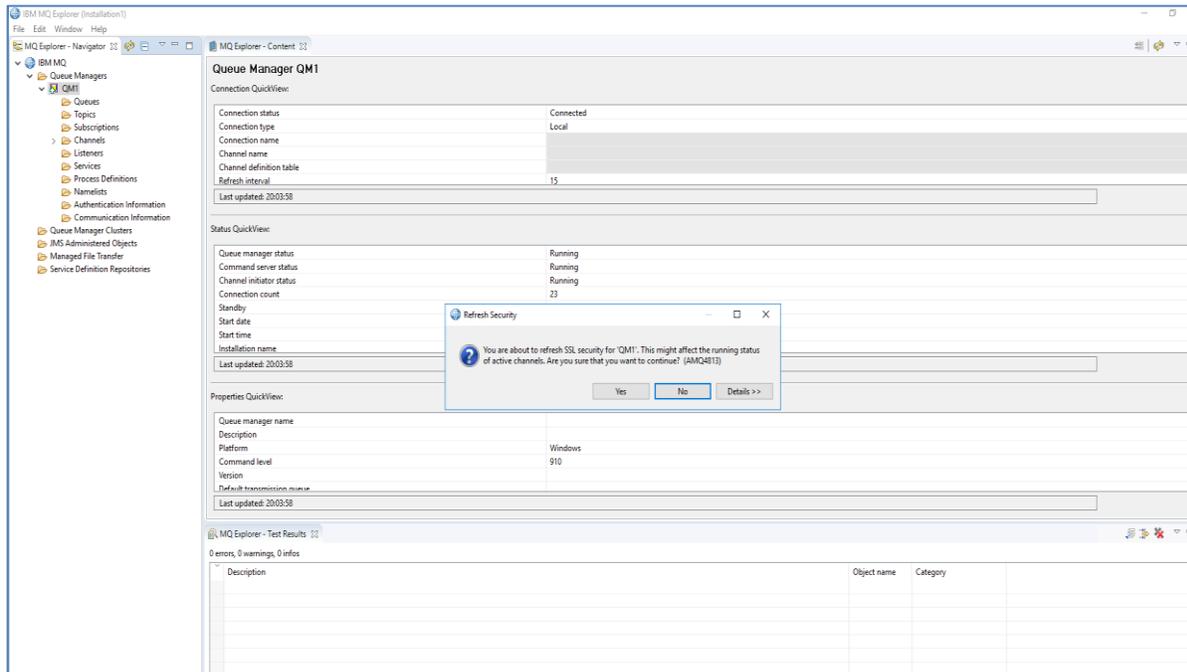
- In **Queue Manager-Properties** window, click **SSL** from the menu on the right side and then **Configure...** under the **Cryptographic hardware** section. Select **other (PKCS11)** and enter the Driver path `C:\Program Files\SafeNet\LunaClient\cryptoki.dll` for Windows and `/usr/safenet/lunaclient/lib/libCryptoki2_64.so` for Linux, followed by **Token label** and **Token password**. After filling all the details, click **OK** and then click **Apply**. When details are saved, close the **SSL** properties window.



- Right Click on Queue Manager and click **Security > Refresh SSL....**



6. A message will pop up to ensure that you are refreshing the SSL security. Click **Yes** to refresh the SSL settings.



7. Run MQSC commands for queue manager.

**Windows:**

```
C:\Program Files\IBM\MQ\bin>runmqsc.exe QM1
```

**Linux:**

```
$ /opt/mqm/bin/runmqsc QM1
```

8. Verify the SSLCRYP and SSLKEYR value.

```
DISPLAY QMGR
```

```
SSLCRYP(GSK_PKCS11=C:\Program  
Files\SafeNet\LunaClient\cryptoki.dll;ibmmq;*****;)
```

```
SSLKEYR(C:\ProgramData\IBM\MQ\qmgrs\QM1\ssl\key)
```

9. On QM1 queue manager, create a listener for the connection channel.

```
DEFINE LISTENER(QM1.TCP) TRPTYPE(TCP) PORT(1414) CONTROL(QMGR)
```

Where LISTENER is the user-defined name, such as QM1.TCP.

10. Start the listener.

```
START LISTENER(QM1.TCP)
```

11. Check the status of listener.

```
DISPLAY LSSTATUS(QM1.TCP)
```

12. Create server connection channel.

```
DEFINE CHANNEL(C1.TO.QM1) CHLTYPE(SVRCONN) TRPTYPE(TCP)  
MCAUSER('MUSR_MQADMIN') SSLCAUTH(REQUIRED)
```

```
SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA256) DESCR('Server channel using SSL
from C1 to QM1')

DEFINE CHANNEL(C1.TO.QM1) CHLTYPE(SVRCONN) TRPTYPE(TCP) MCAUSER('mqm')
SSLCAUTH(REQUIRED) SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA256) DESCR('Server
channel using SSL from C1 to QM1')
```

Where:

- CHANNEL is the user-defined channel name.
- MCAUSER is the user added in the MQM group.

### 13. Start the channel.

```
START CHANNEL(C1.TO.QM1)
```

### 14. Create a client connection channel.

```
DEFINE CHANNEL(C1.TO.QM1) CHLTYPE(CLNTCONN) TRPTYPE(TCP)
CONNAME('HSMNOI1INT-MA01.noidalab.local') QMNAME(QM1)
SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA256) DESCR('Client channel using SSL
from C1 to QM1')
```

Here, CONNAME is the hostname or IP of the MQ Server.

**NOTE:** Ensure that channel name and SSL cipher for client connection channel match the server connection channel.

### 15. Create channel authentication record to authorize the client when it connects to MQ Server.

```
SET CHLAUTH(C1.TO.QM1) TYPE(ADDRESSMAP) ADDRESS('HSMNOI1INT-
MA02.noidalab.local') MCAUSER('MUSR_MQADMIN')

SET CHLAUTH(C1.TO.QM1) TYPE(ADDRESSMAP) ADDRESS('HSMNOI1INT-
MA02.noidalab.local') MCAUSER('mqm')
```

Where:

- ADDRESS is the hostname or IP of the MQ Client.
- MCAUSER is the user authorized to use channel.

**NOTE:** For channel authentication type other than ADDRESSMAP, refer the IBM MQ Documentation.

### 16. Create a local queue on QM1.

```
DEFINE QLOCAL(QM1.LQ)
```

Here, QLOCAL is the user defined local queue.

### 17. To close MQSC, type `END` and then press Enter.

18. Restart the queue manager to apply all the changes. To restart, run the following commands:

**Windows:**

```
C:\Program Files\IBM\MQ\bin>endmqm.exe QM1
C:\Program Files\IBM\MQ\bin>strmqm.exe QM1
```

**Linux:**

```
$ /opt/mqm/bin/endmqm QM1
$ /opt/mqm/bin/strmqm QM1
```

## Configure MQ Client for SSL/TLS to use Luna HSM Keys

MQ Client SSL keys and certificate are already generated on the Luna HSM. Now you need to configure the MQ Client to use these keys and certificate while establishing the SSL connection with MQ Server. To configure the client, perform the following steps:

1. Log on to the IBM MQ Client using the Administrator account or user added in mqm group.
2. To configure Hardware Cryptographic Token, add the SSL stanza in the mqclient.ini file available at the C:\ProgramData\IBM\MQ or /var/mqm directory.

**Windows:**

SSL:

```
SSLCryptoHardware=GSK_PKCS11=C:\Program
Files\SafeNet\LunaClient\cryptoki.dll;ibmmq;userpin1;SYMMETRIC_CIPHER_OFF
SSLKeyRepository=C:\ProgramData\IBM\MQ\key
```

**Linux:**

SSL:

```
SSLCryptoHardware=GSK_PKCS11=/usr/safenet/lunaclient/lib/libCryptoki2_64
.so\;ibmmq\;userpin1\;SYMMETRIC_CIPHER_OFF
SSLKeyRepository=/var/mqm/key
```

Where:

- SSLCryptoHardware is a string in the format: GSK\_PKCS11 = driver path and filename;token label;token password;symmetric cipher setting and
  - SSLKeyRepository is the location of key repository that holds the user's digital certificate in stem format. That is, it includes the full path and the file name without an extension.
3. Copy the Client Channel Definition Table (AMQCLCHL.TAB) from MQ Server to MQ Client. The Client Channel Definition Table is located at the following location on the MQ server:

**Windows:**

```
C:\ProgramData\IBM\MQ\qmgrs\QM1\@ipcc\
```

**Linux:**

```
/var/mqm/qmgrs/QM1/@ipcc/
```

Copy the AMQCLCHL.TAB file to MQ Client at "C:\ProgramData\IBM\MQ" or "/var/mqm"

## Configuring SSL/TLS for IBM WebSphere MQ using Luna HSM

The TLS (Transport Layer Security) protocol enables queue managers to communicate securely with other queue managers or clients. When a queue manager connects with another queue manager or client, the two carry out a standard TLS exchange of certificates and validation checks. If the validation is successful, the connection is established. To achieve this, the queue managers and clients, as well as the channels that they use, must be configured with appropriate certificate settings.

When messages are sent from one queue manager to another queue manager or client along a channel, the data is generally encrypted using a session key that has been established during the certificate exchange. To achieve this, you must configure the channels that you use with appropriate cipher specs.

You have already generated the certificates on Luna HSM and have configured both queue manager and clients to use the TLS connection through the channel created and authenticated using Channel Authentication Record. To verify SSL/TLS connectivity between MQ server and MQ client:

1. Log on to the IBM MQ Client through the Administrator account or a user added to mqm group.
2. Open the command prompt and set the following environment variables:

### **Windows:**

```
set MQCHLLIB=C:\ProgramData\IBM\MQ
set MQCHLTAB=AMQCLCHL.TAB
set MQSAMP_USER_ID=MUSR_MQADMIN
```

### **Linux:**

```
export MQCHLLIB=/var/mqm
export MQCHLTAB=AMQCLCHL.TAB
export MQSAMP_USER_ID=mqm
```

Where:

- MQCHLLIB is the location of the Client Channel Definition Table.
- MQCHLTAB is the Client Channel Definition Table copied from the MQ Server.
- MQSAMP\_USER\_ID is the user authorized in MQ Server channel authentication record.

3. Run the following command to create the SSL connection from client to server and put messages in the MQ Server queue.

**Windows:**

```
C:\Program Files\IBM\MQ\bin>amqsputc.exe QM1.LQ QM1
```

**Linux:**

```
/opt/mqm/samp/bin/amqsputc QM1.LQ QM1
```

```
C:\Program Files\IBM\MQ\bin>amqsputc.exe QM1.LQ QM1
Sample AMQSPUT0 start
Enter password: *****
target queue is QM1.LQ
Hiiii
MQ Server Are You Alive!!!
_
```

The messages you type here will be delivered to MQ Server securely using the established SSL/TLS connection. MQ Server can access the messages received from MQ Client.

4. Log on to IBM MQ Server using the Administrator account.
5. Open the command prompt and run the following command to get the message sent by client:

**Windows:**

```
C:\Program Files\IBM\MQ\bin>amqsget.exe QM1.LQ QM1
```

**Linux:**

```
/opt/mqm/samp/bin/amqsget QM1.LQ QM1
```

```
C:\Program Files\IBM\MQ\bin>amqsget.exe QM1.LQ QM1
Sample AMQSGET0 start
message <Hiiii>
message <MQ Server Are You Alive!!!>
no more messages
Sample AMQSGET0 end

C:\Program Files\IBM\MQ\bin>_
```

This completes the integration of IBM WebSphere MQ with SafeNet Luna HSM by securing the SSL/TLS authentication certificates/keys on Luna HSM.

---

## Contacting Customer Support

---

If you encounter a problem while installing, registering, or operating this product, refer to the documentation. If you cannot resolve the issue, contact your supplier or [Thales Customer Support](#). Thales Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

### Customer Support Portal

The Customer Support Portal, at <https://supportportal.thalesgroup.com>, is a database where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable repository of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

**NOTE:** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

### Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Thales Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.