

Using Multiple Certificates in IBM MQ

Messaging Administrator

Summary: Implementing multiple queue manager certificates and host names

Lab 7 - Using Multiple Certificates in IBM MQ

The objective of these exercises is to demonstrate the multiple certificate feature of IBM MQ and to show how different channels can use different certificates.

You will create two new queue managers, QM8 and QMC, for testing SSL channels.

Initially, by setting the queue manager CERTLBL property, we will configure QMC to use a certificate with label 'ALL QMGR cert'.

We will then create a channel which will use a different certificate label 'QM8 CHL cert' (by setting the CERTLBL property on the receiver channel).

Finally you will create a second channel which will use the queue manager certificate label 'ALL QMGR cert'.

CERTLBL refers to the labels inside the key repository. We can use iKeyMan to see this. Any label can be assigned by the MQ administrator and the label does not need to be related to the certificate. In this example the CN attribute of the certificates and the certificate labels happen to be the same for ease of use, but there is no requirement for this in general. Good practice for Distinguished Names is to choose certificate labels that 'relate to' the certificates DN.

[View an overview of using Multiple Certificates for TLS Channels](#) ↗

You should be logged in as ibmdemo / passw0rd and MQ Explorer should be running.

Lab Setup

1. Once the Windows VMware image starts up, click the terminal icon to get to the Windows desktop.

PoT Messaging - Base MQ

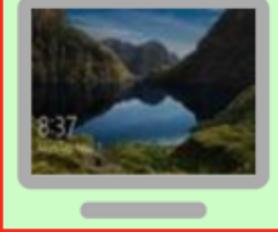
Running: an hour (created: 7 days ago)
Template for MQ portion of Messaging PoT. Windows10 Enterprise license applied.

Settings: Tags:

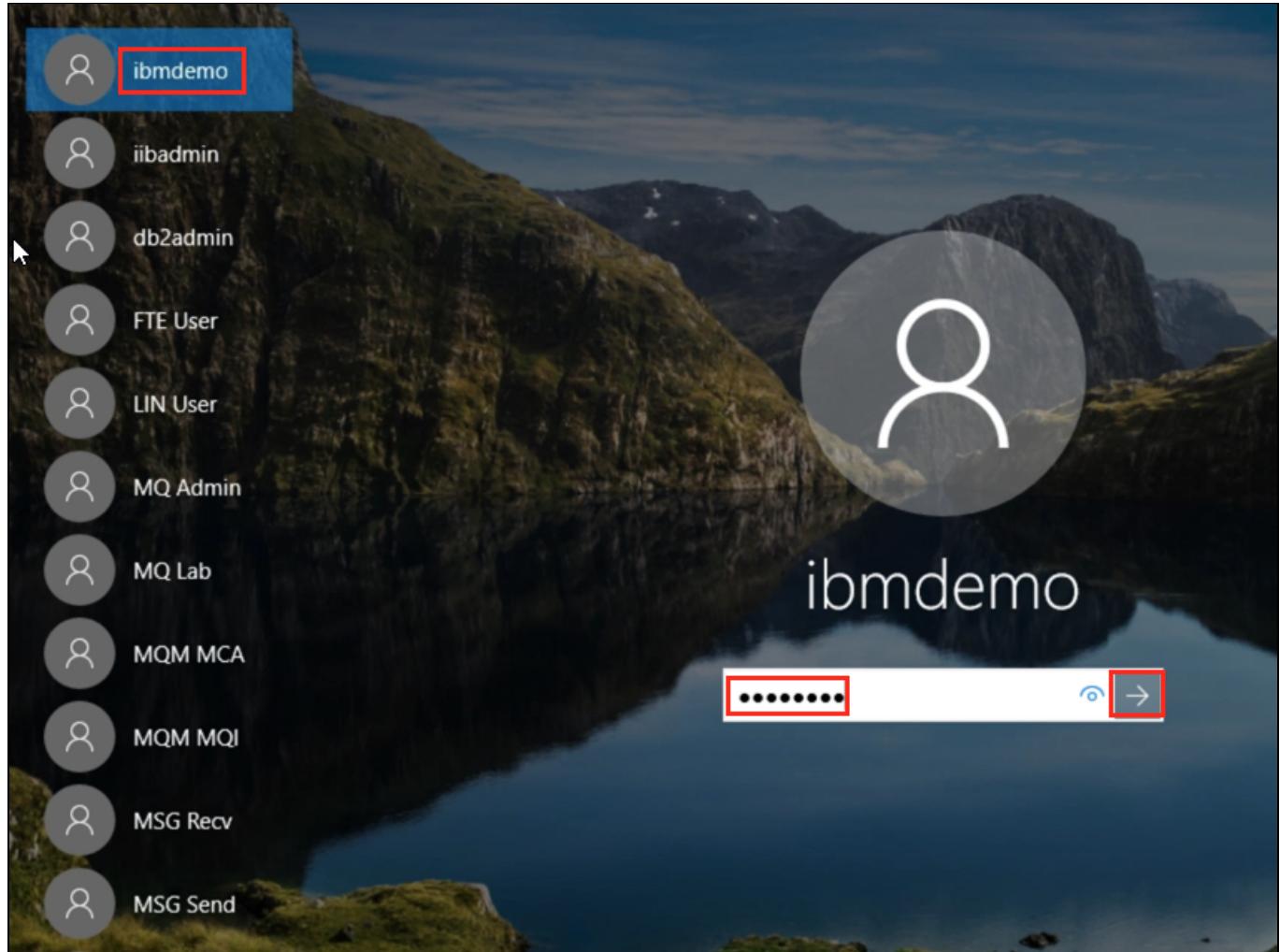
Region/Owner US-Central Jack Carnes	VMs (1): Settings SVMs: 4	Storage: 100 GB	Networking: Settings Networks: 1 ▾ Pub. services: 0 ▾
---	--	-----------------	---

VMs (1) Containers (0) Sharing Portals Network Topology Labels (2) Activity

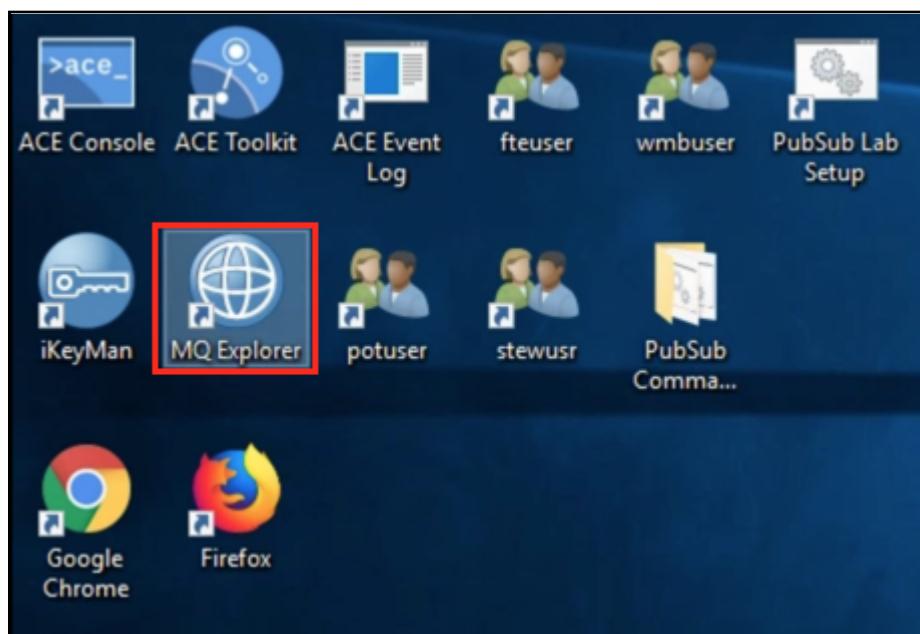
▶ || ■ ⏻ Sort by date created ↑ ↓

Running		■	⏻	RDP	
<input checked="" type="checkbox"/> Windows 10 x64 ✎ Endpoints: 1 (host-1 - 10.0.0.2)					
					
SVMS	RAM	CPUS	STORAGE		
4	4 GB	2	100 GB		
CPU 4	RAM 0	DISK 0	NET	⚙️	X

2. Sign in as **ibmdemo** by clicking the icon. Enter **passw0rd** for the password and click the right arrow.

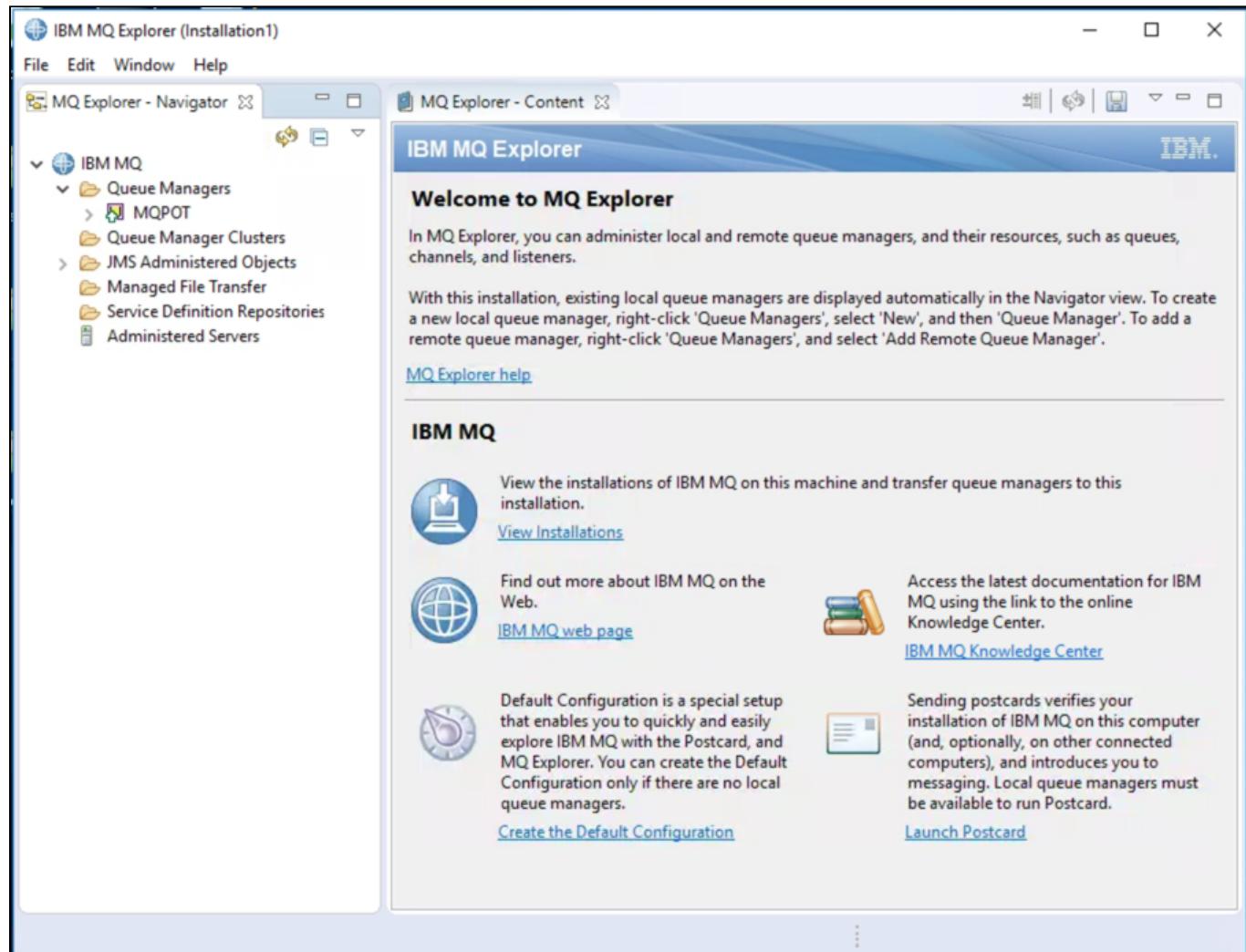


3. The indicated icon represents IBM MQ on this system.

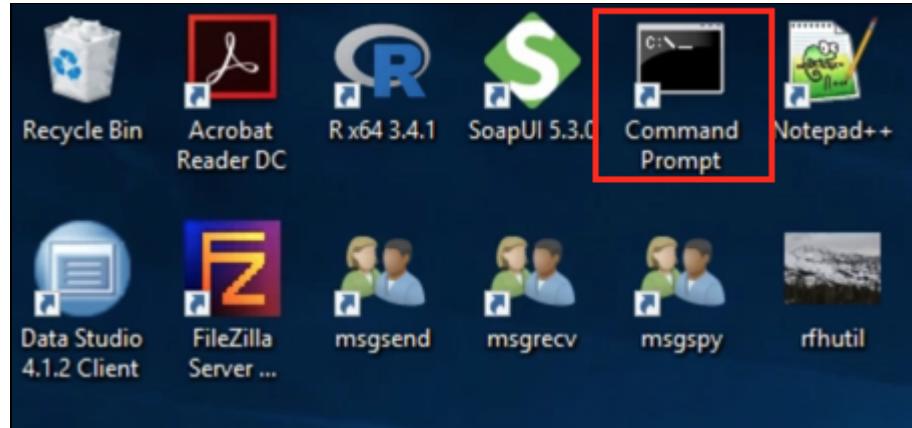


4. Start the MQ Explorer by double-clicking the icon and selecting.
5. The welcome screen provides a nice selection of resources for the product. Note the various options on the Welcome screen and explore them if you would like. The first time you launch IBM MQ Explorer after an install of IBM MQ this Welcome screen will be displayed automatically.

Note: You may have different queue managers on your MQ Explorer depending on what labs have completed.



6. Open a command prompt by double-clicking the icon on the desktop.



7. Run the `dspmqver` command to confirm the version of MQ installed.

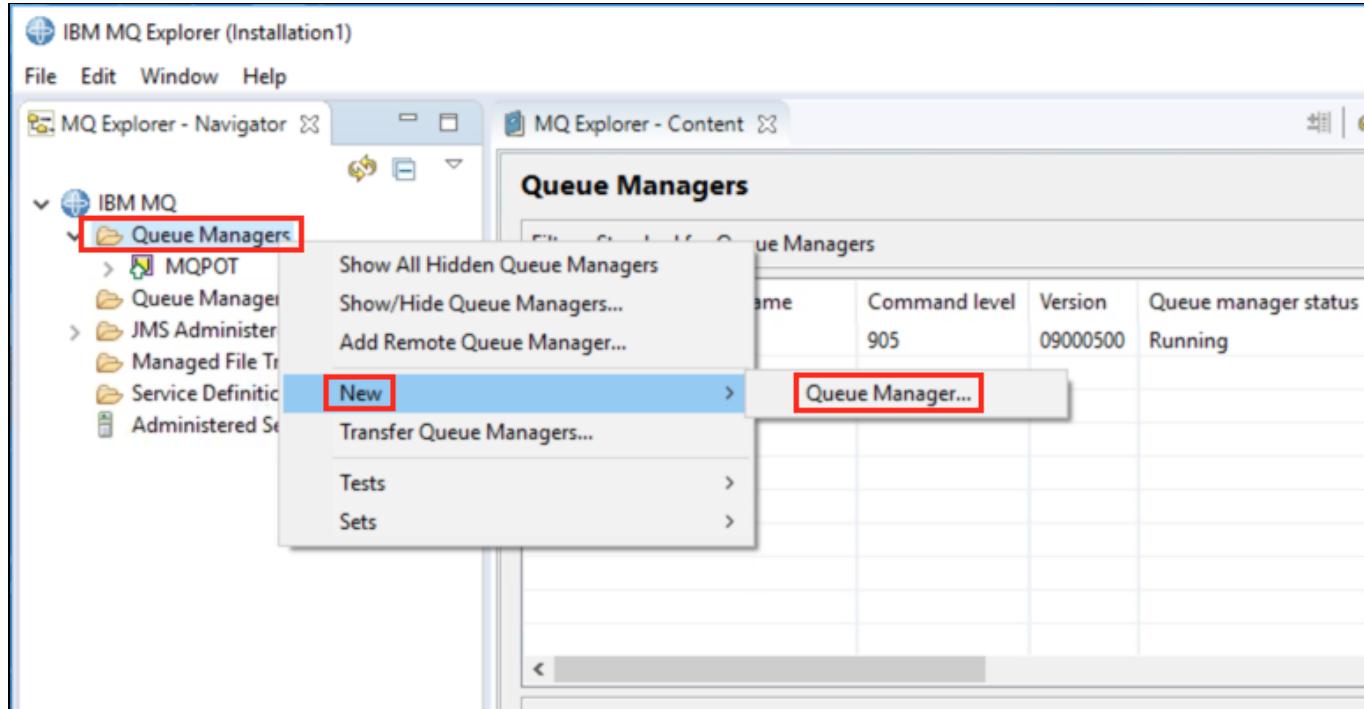
```
Microsoft Windows [Version 10.0.16299.402]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\ibmdemo.DESKTOP-6DS00H2>dspmqver
Name:           IBM MQ
Version:        9.0.5.0
Level:          p905-L180305.1
BuildType:      IKAP - (Production)
Platform:       IBM MQ for Windows (x64 platform)
Mode:           64-bit
O/S:            Windows 10 Enterprise x64 Edition, Build 16299
InstName:       Installation1
InstDesc:
Primary:        Yes
InstPath:       C:\Program Files\IBM\MQ
DataPath:       C:\ProgramData\IBM\MQ
MaxCmdLevel:   905
LicenseType:    Production

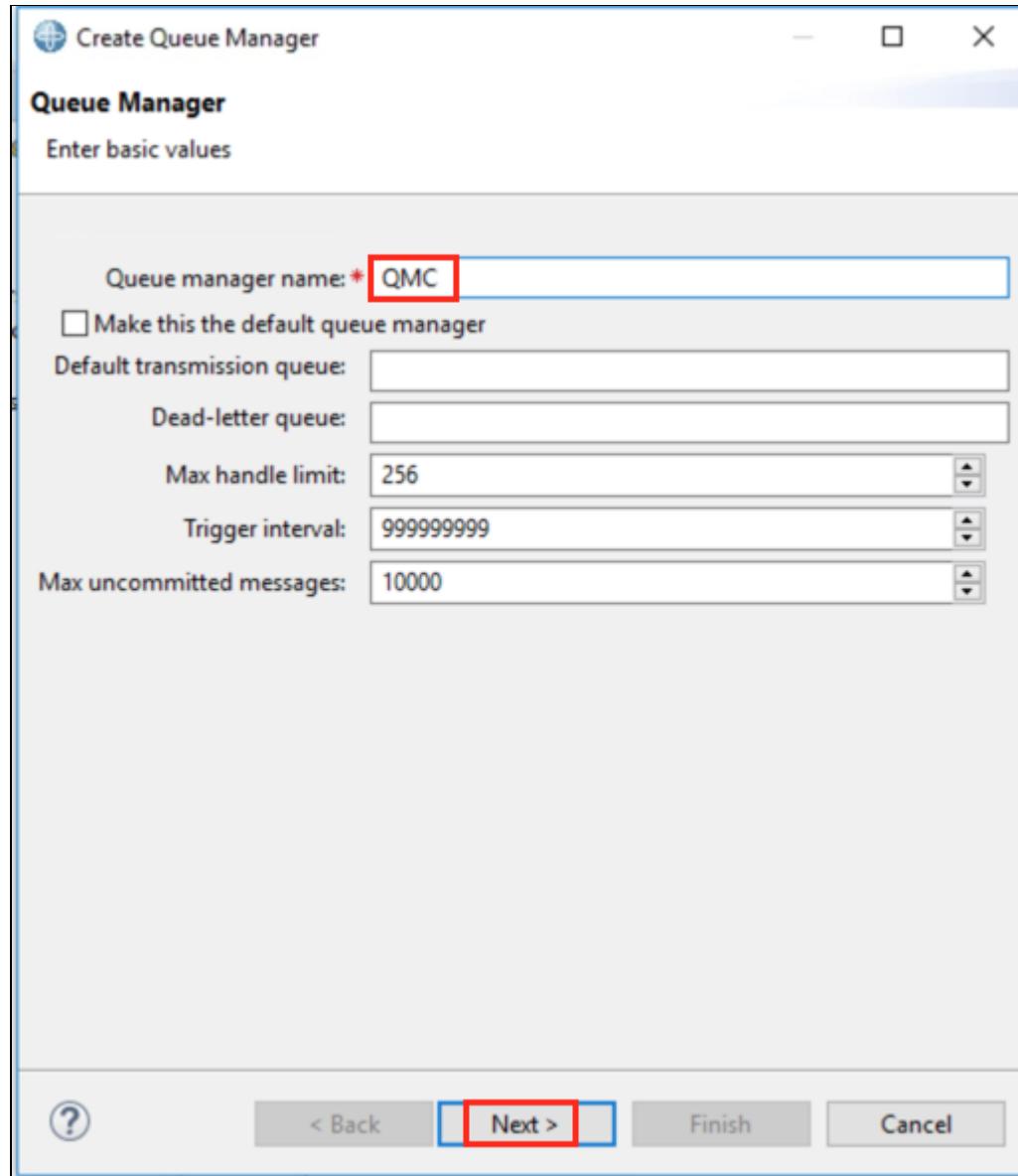
C:\Users\ibmdemo.DESKTOP-6DS00H2>
```

Create new queue managers

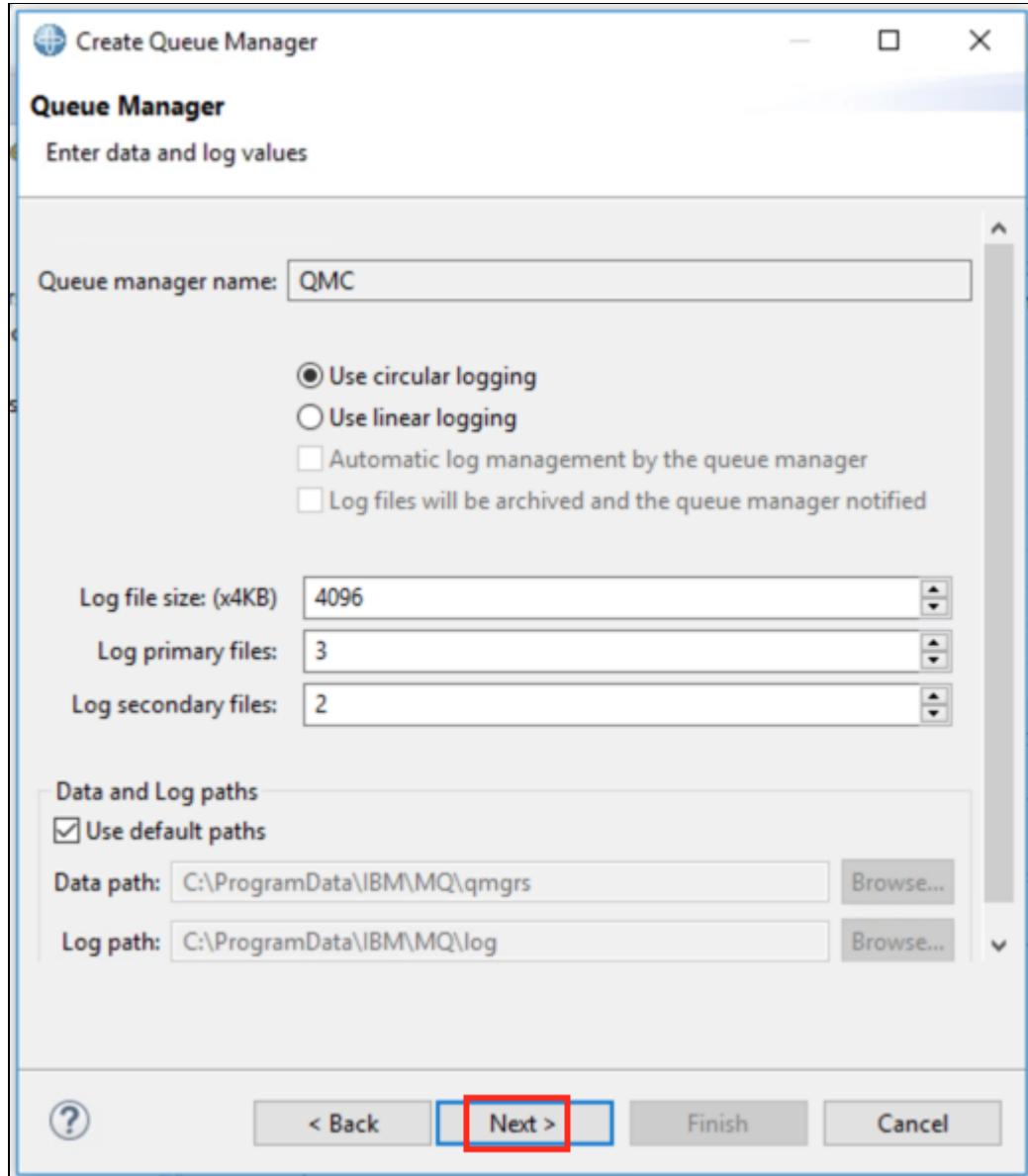
1. On MQ Explorer, right click on the ‘Queue Managers’ folder and choose ‘New’ and ‘Queue Manager’.



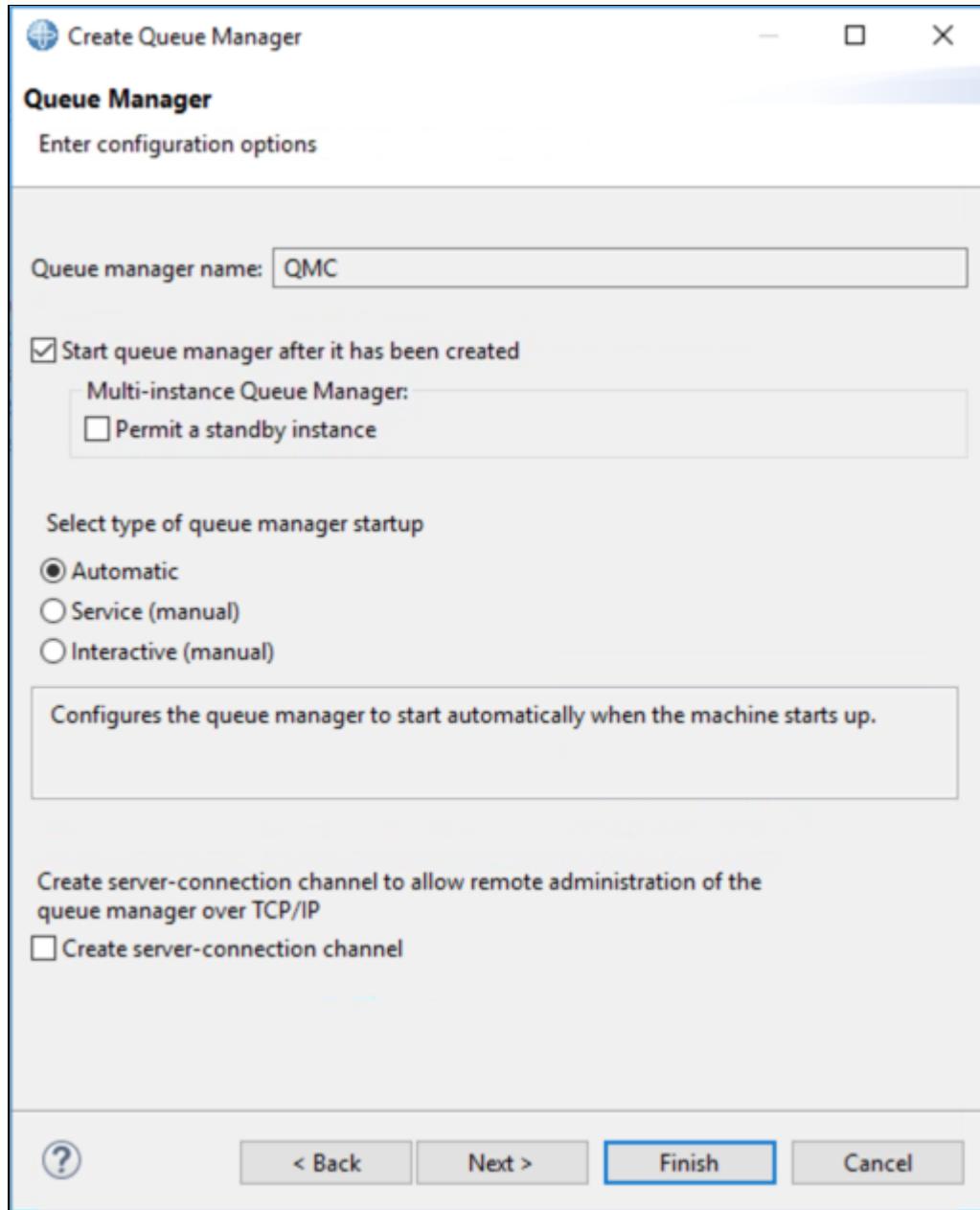
2. Provide 'Queue manager name' as 'QMC' and click 'Next'.



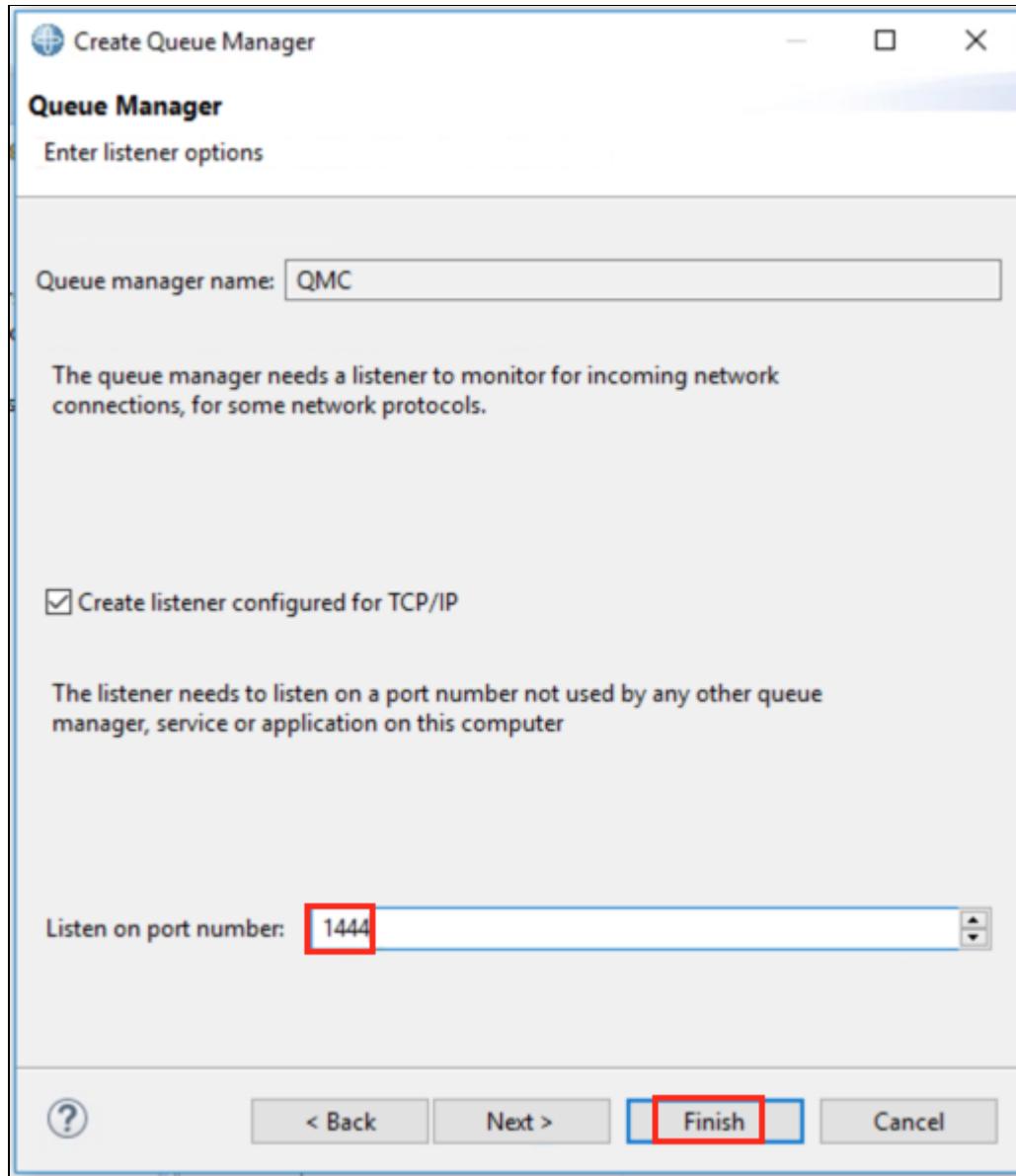
3. Accept the default values and click the 'Next' button.



4. Accept the default values and click the 'Next' button.



5. Provide the listener port as '1444' and click on 'Finish' button.



6. Alternatively, you can use the command prompt to create the queue manager by providing the following command.

```
crtmqm QMC
```

Also, start the queue manager QM8 using the command below.

```
strmqm QMC
```

If the queue manager is created on the command prompt, ensure that you create a listener by using the runmqsc editor provided by IBM MQ.

The command to create the listener is:

```
DEFINE LISTENER('LISTENER.TCP') TRPTYPE(TCP) PORT(1444)
```

Start the listener using the command below:

START LISTENER('LISTENER.TCP')

```
Command Prompt

C:\Users\ibmdemo.DESKTOP-6DSOOH2>runmqsc QMC
5724-H72 (C) Copyright IBM Corp. 1994, 2018.
Starting MQSC for queue manager QMC.

DEFINE LISTENER('LISTENER.TCP') TRPTYPE(TCP) PORT(1444) REPLACE
  1 : DEFINE LISTENER('LISTENER.TCP') TRPTYPE(TCP) PORT(1444) REPLACE
AMQ8626I: IBM MQ listener created.
START LISTENER('LISTENER.TCP')
  2 : START LISTENER('LISTENER.TCP')
AMQ8730W: Listener already active.
END
  3 : END
2 MQSC commands read.
No commands have a syntax error.
One valid MQSC command could not be processed.

C:\Users\ibmdemo.DESKTOP-6DSOOH2>
```

7. Repeat the above steps 1 - 5 to create another queue manager named QM8 using port 1454.

Exercise overview

Configure QM8 and QMC to use SSL

These are the steps you will perform:

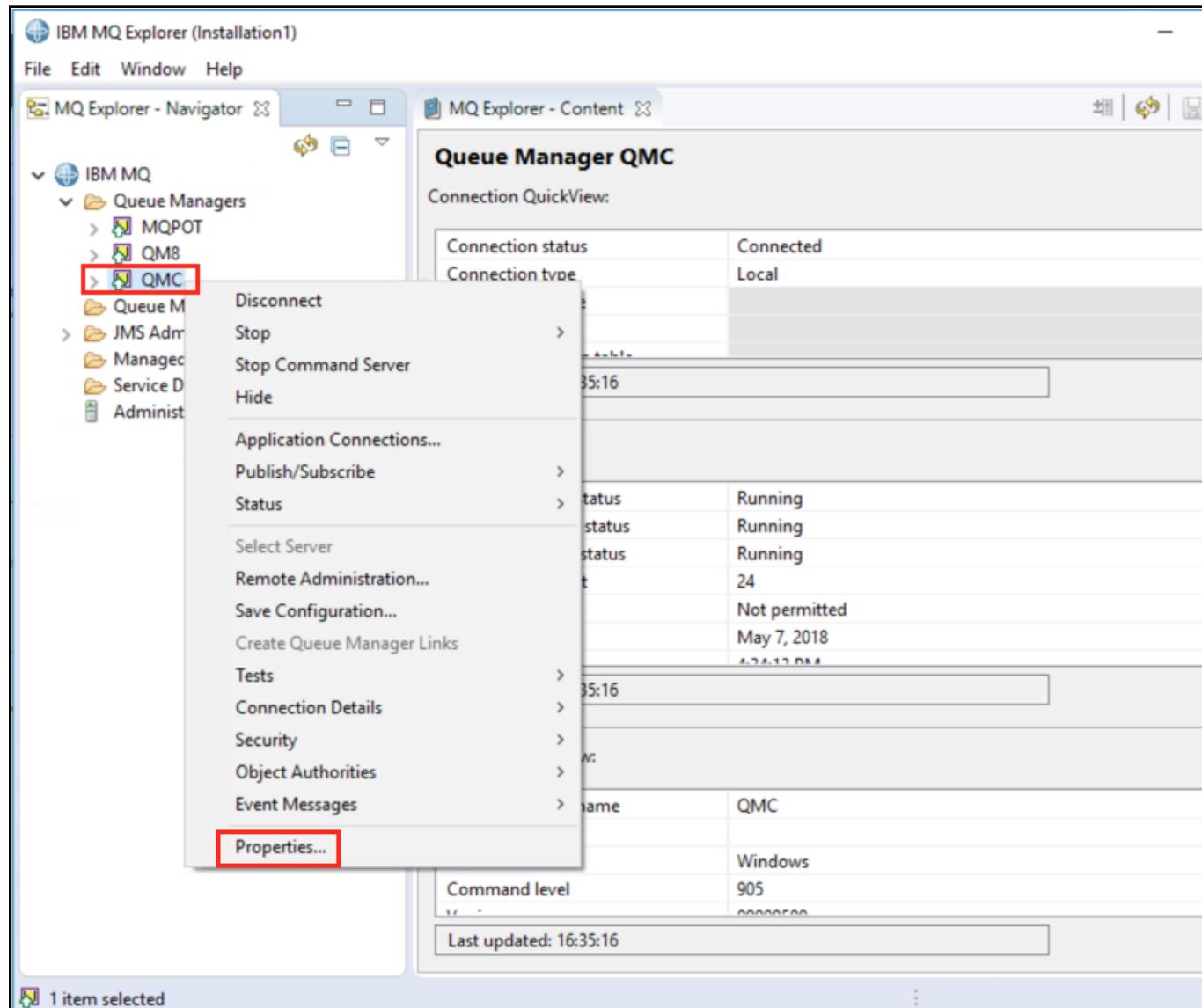
- Configure queue manager QMC to use SSL
- Configure QMC queue manager SSL properties to specify the keystore
- Configure QM8 SSL properties
- Certificates are supplied in C:\PoT-messaging\STUDENT\Lab7 and will be added to the keystores
- Define a SDR channel QM8.TO.QMC on MQPOT
- Define the RCVR channel on QMC
- Create a new SDR RCVR using the certificate specified in RCVR queue managers CERTLABL

Configure QMC queue manager SSL properties

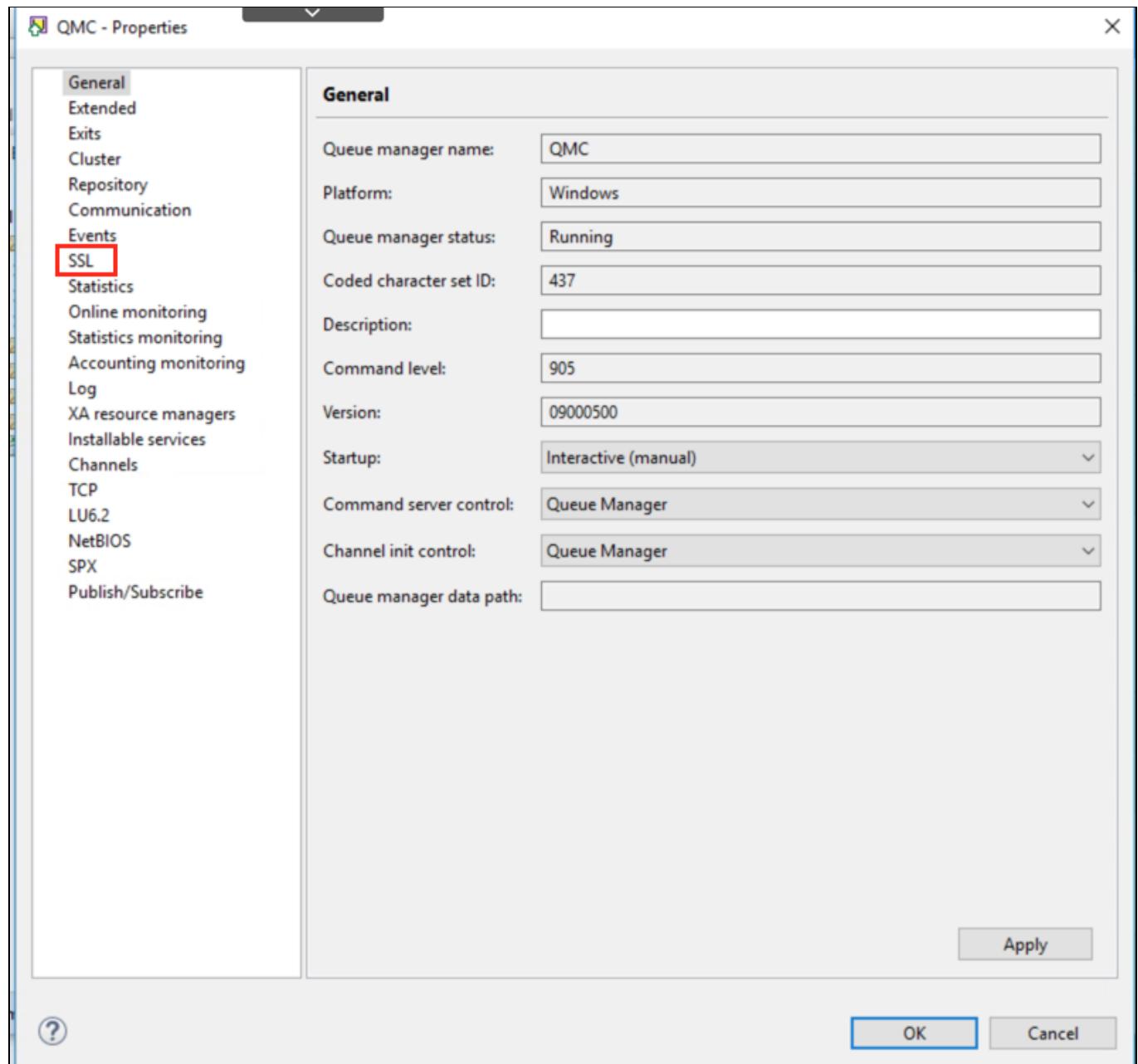
On QMC we are going to specify the certificate this Queue Manager will use. This is achieved by setting the Queue Manager SSL property CERTLBL.

To configure QMC queue manager SSL properties:

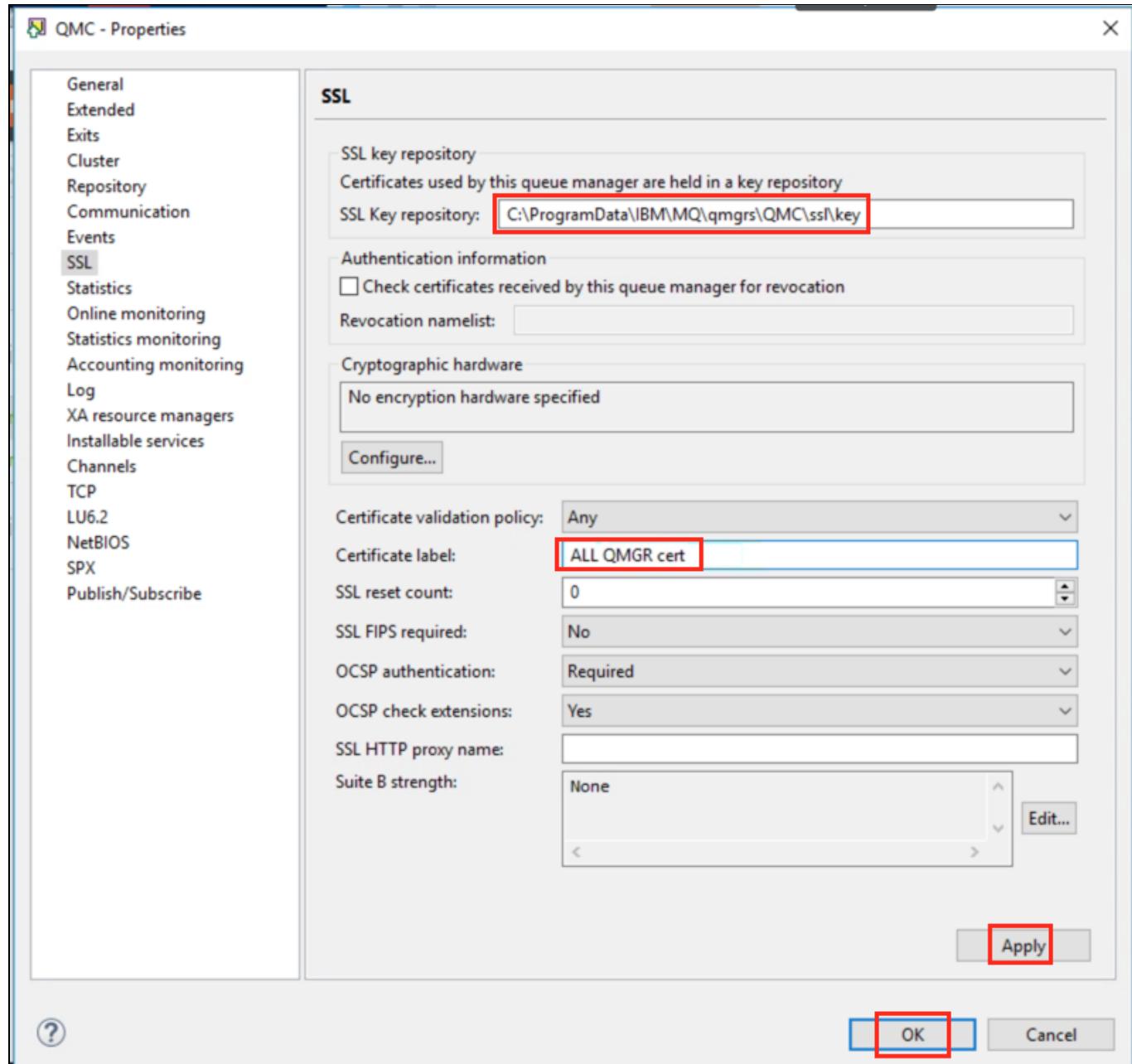
1. In MQ Explorer right click the queue manager name QMC and select Properties.



2. Once the QMC – Properties panel appears, select SSL.



3. Check that the SSL key repository name is C:\ProgramData\IBM\MQ\qmgrs\QMC\ssl\key.
4. Alter the Certificate Label field on QMC to 'ALL QMGR cert'.
5. Select Apply then OK.

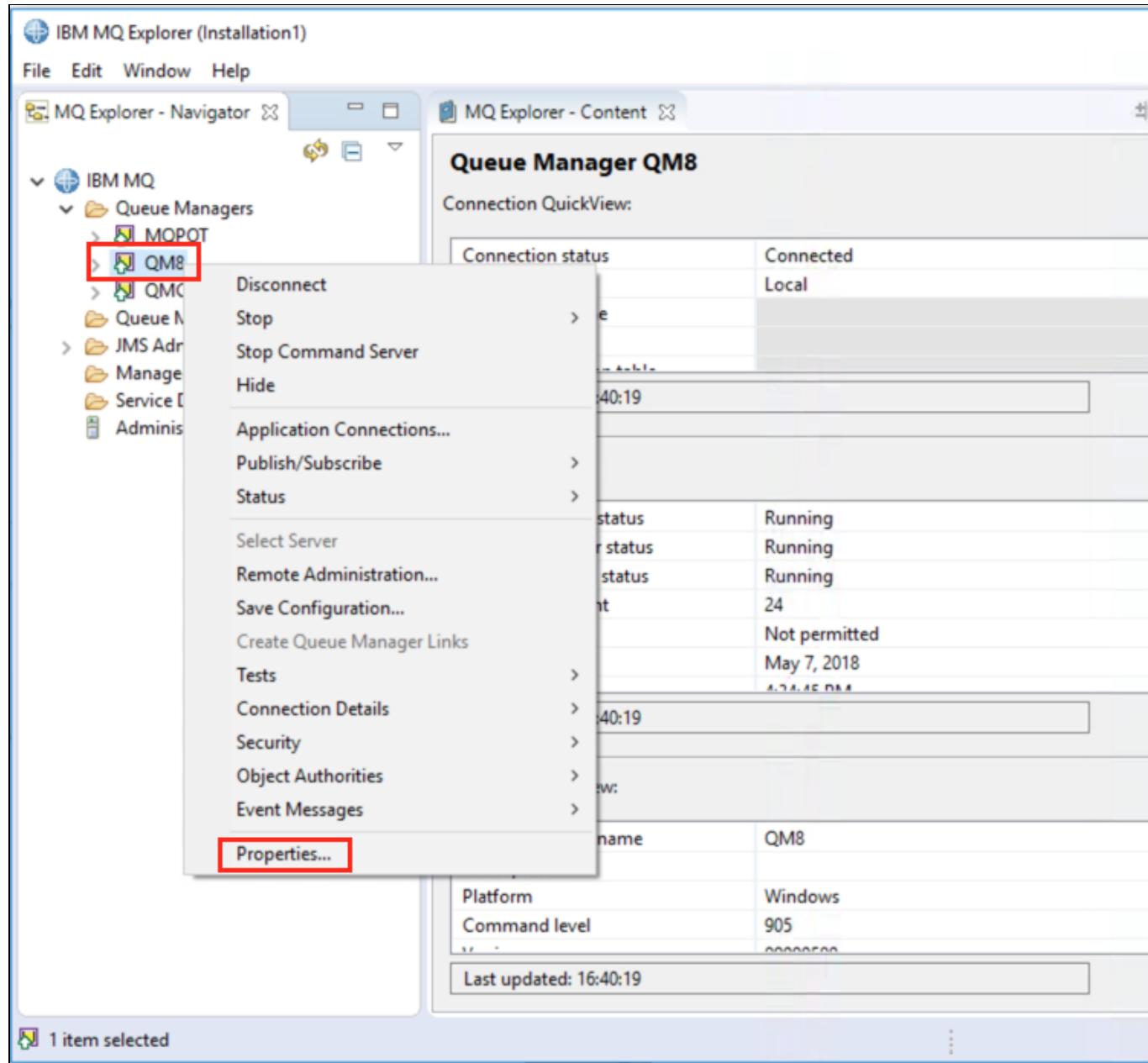


Alternatively, you could use runmqsc command to enter the following command:

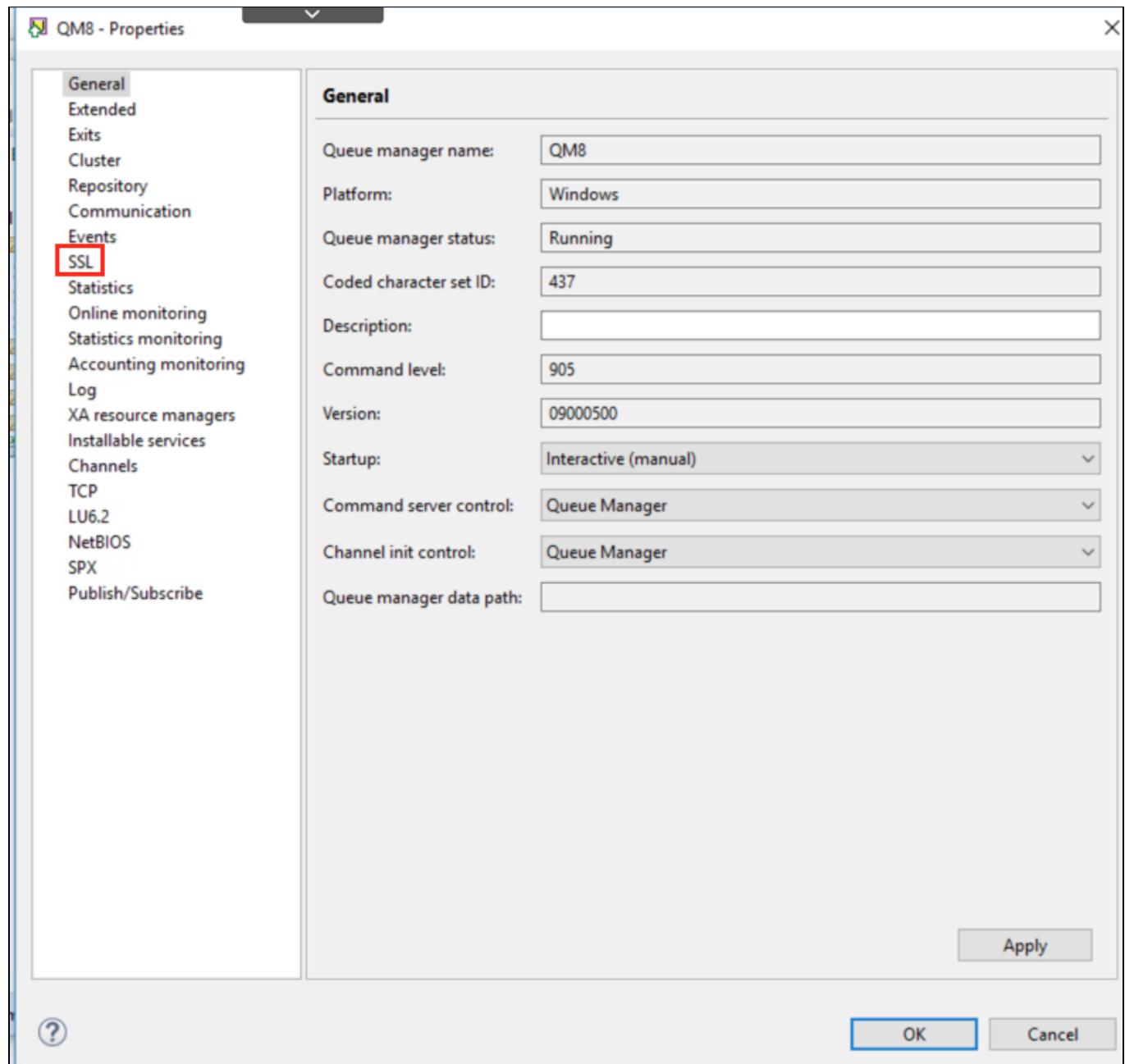
```
ALTER QMGR CERTLBL('ALL QMGR cert')
```

Configure QM8 queue manager SSL properties

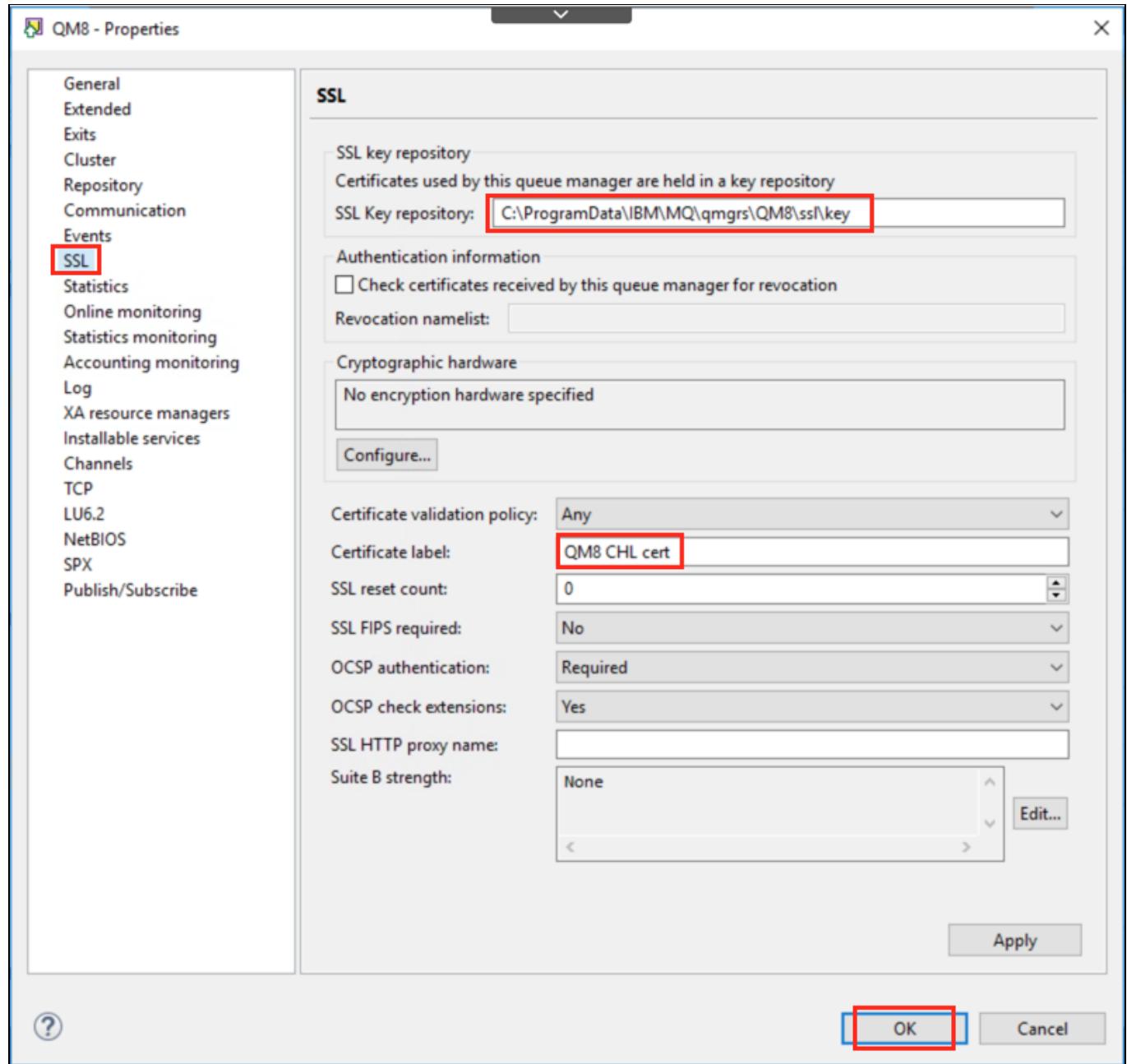
1. In MQ Explorer, right click the queue manager name QM8 and select Properties.



- When the QM8 – Properties panel appears, select SSL.



3. Check the SSL key repository name is C:\ProgramData\IBM\MQ\qmgrs\QM8\ssl\key.
4. Alter the Certificate Label field to 'QM8 CHL cert'.
5. Select Apply then OK.



Alternatively, you could use runmqsc command to enter the following command:

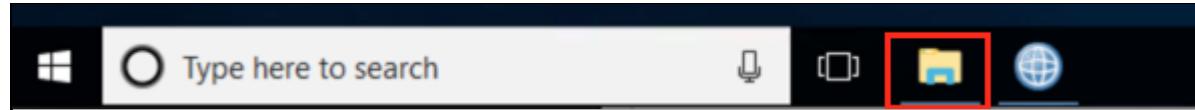
```
ALTER QMGR CERTLBL('QM8 cert')
```

Copy SSL keystore with certificates

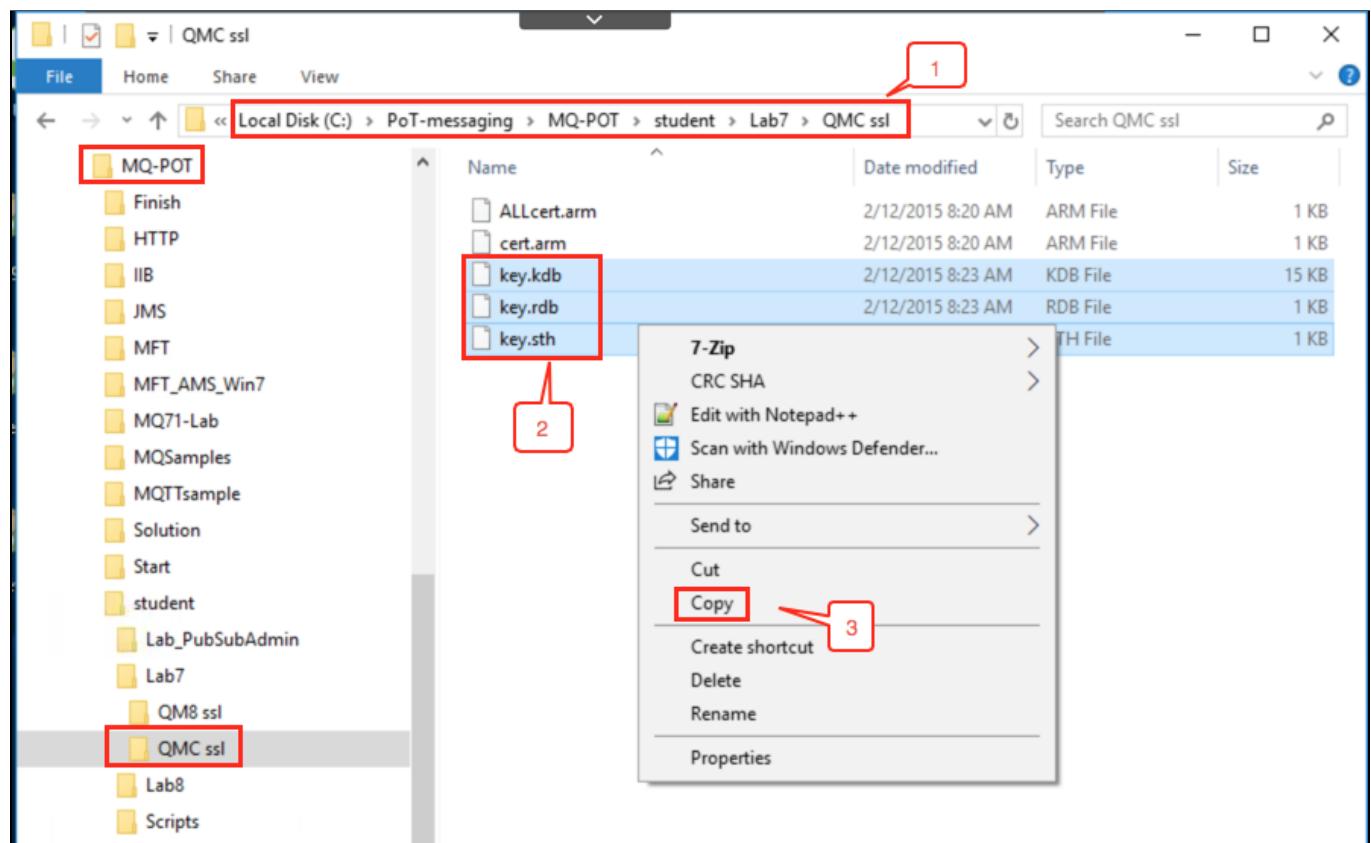
The queue manager's SSL directory should be empty for QM8 and QMC so you need to create this by copying one we have supplied.

For QMC copy the SSL keystore files

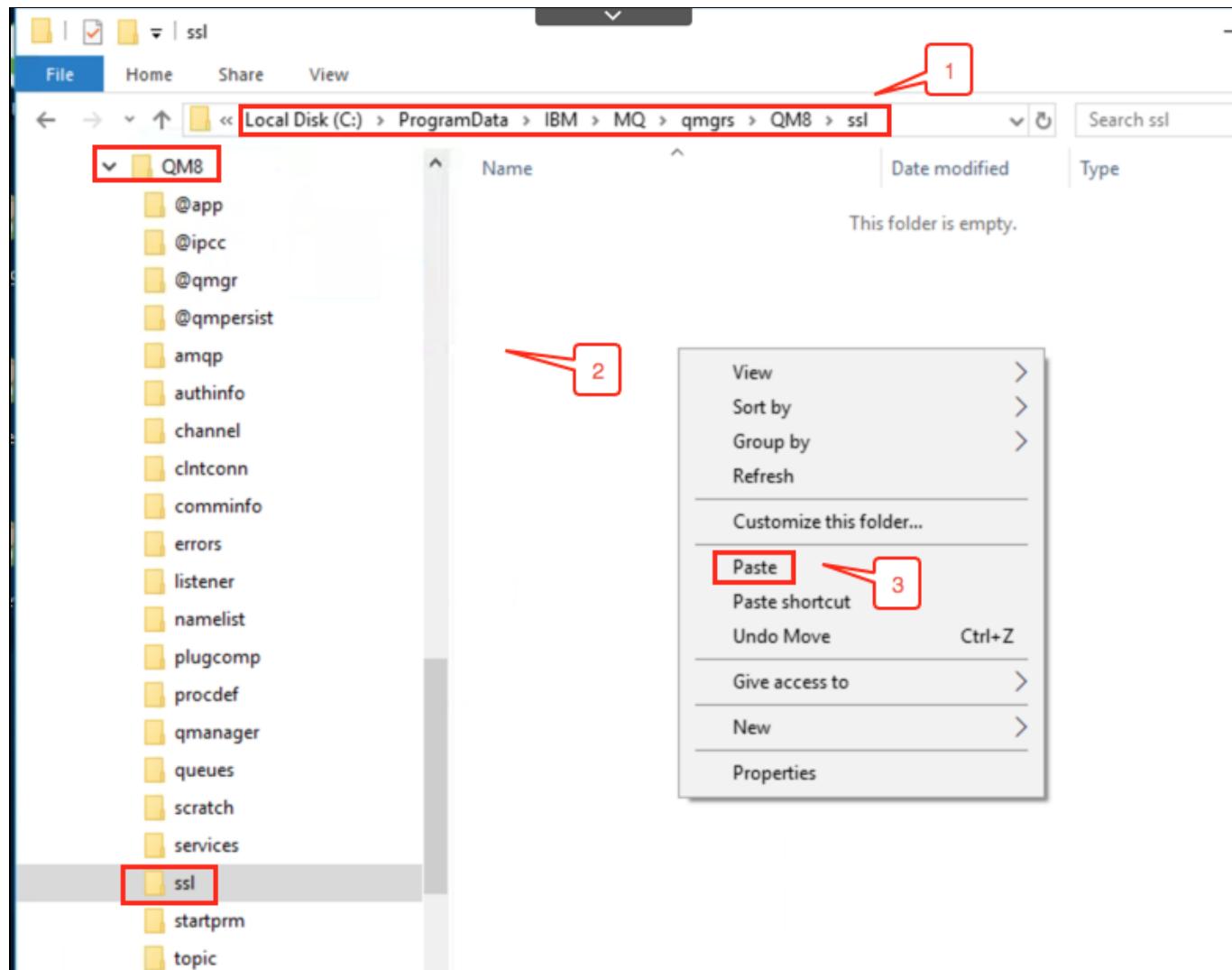
1. Open Windows Explorer by clicking its icon on the task bar.



2. Navigate to 'C:\PoT-messaging\MQ-PoT\student\Lab7\QMC ssl'.
3. Select all the key.* files in the folder. Right-click and select copy.

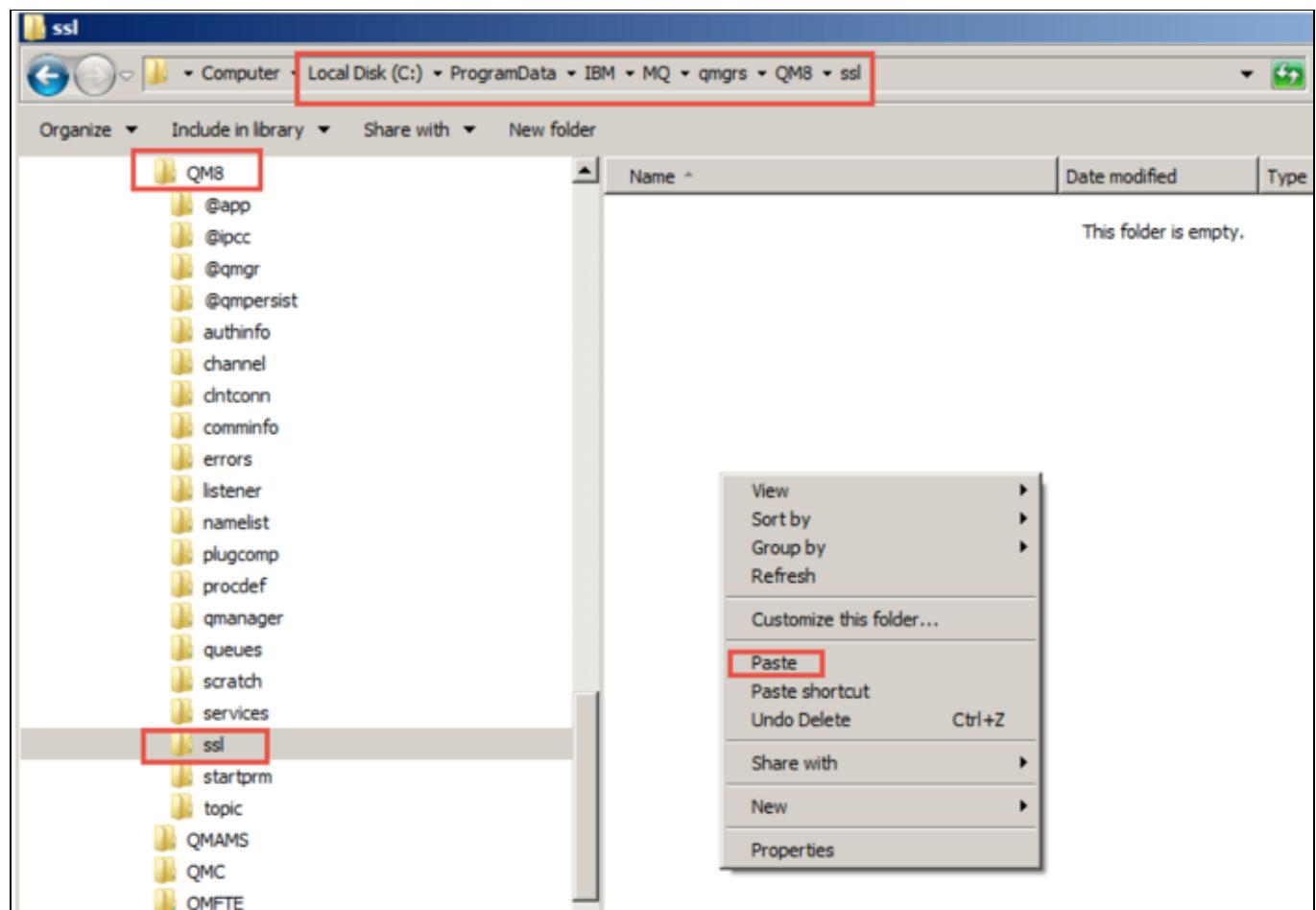
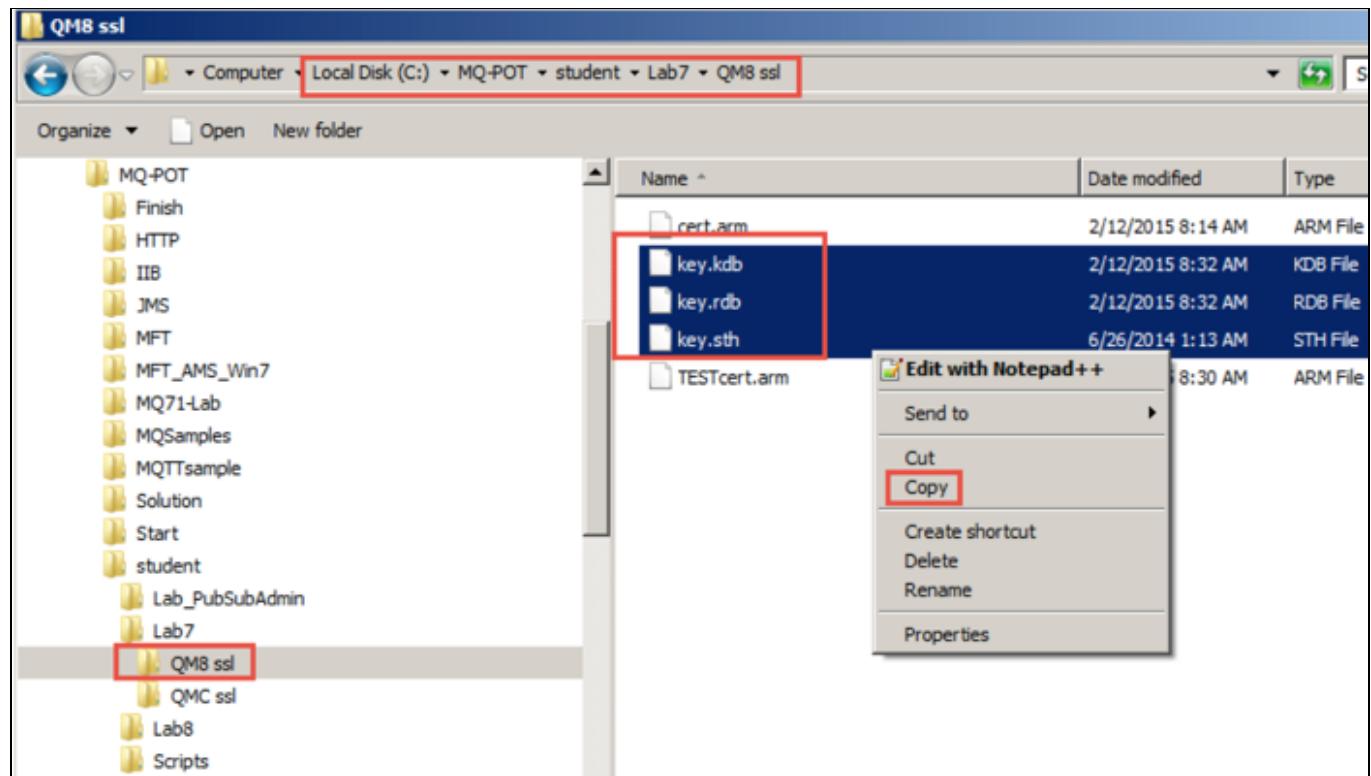


4. Navigate to 'C:\ProgramData\IBM\MQ\qmgrs\QMC\ssl' folder and paste the files into this empty folder.

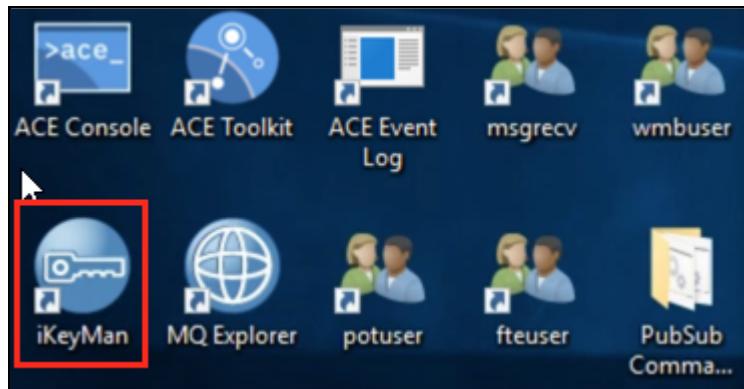


5. To do the same for QM8, repeat Steps 2 – 4 for QM8.

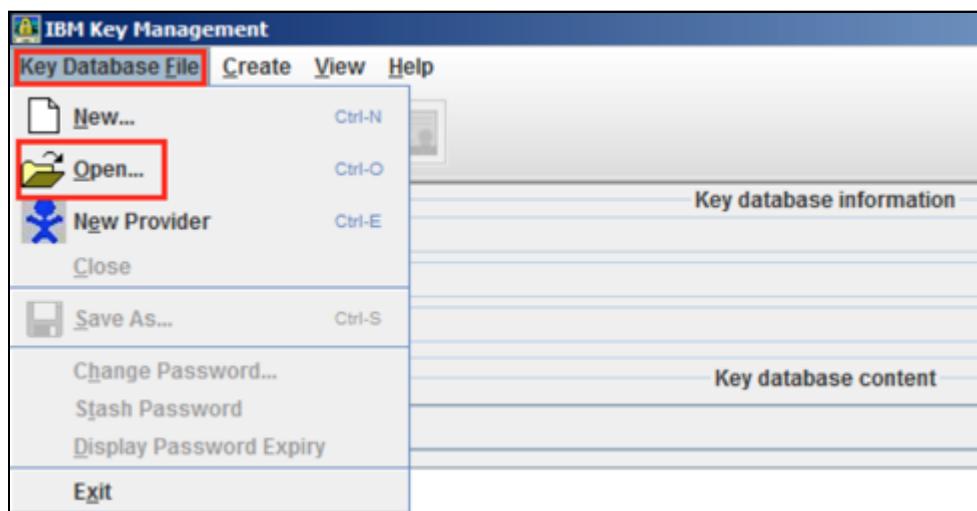
Copy all 3 files from 'C:\PoT-messaging\MQ-POT\student\Lab7\QM8 ssl' into the queue manager's ssl directory 'C:\ProgramData\IBM\MQ\qmgrs\QM8\ssl'.



6. To check the certificates and view the certificate content open ikeyman GUI by double-clicking the icon on the desktop.

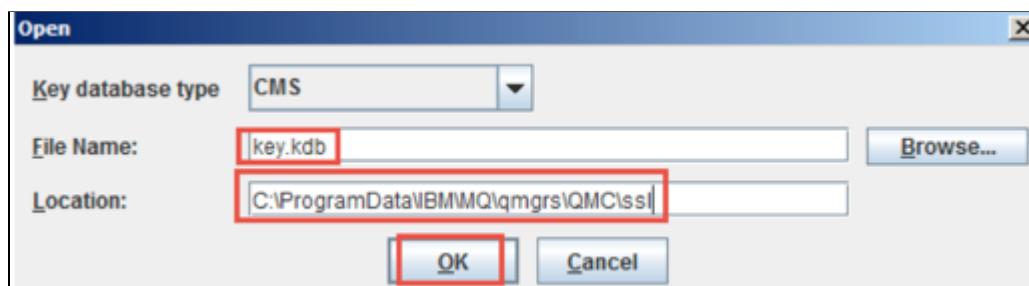


7. Select 'Key Database File', then click Open.

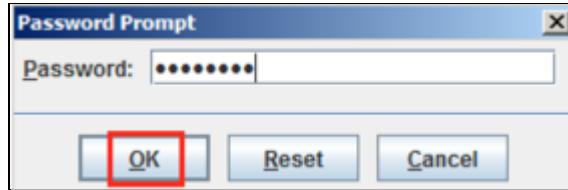


8. Enter the keystore name. For example 'C:\ProgramData\IBM\MQ\qmgrs\QMC\ssl':

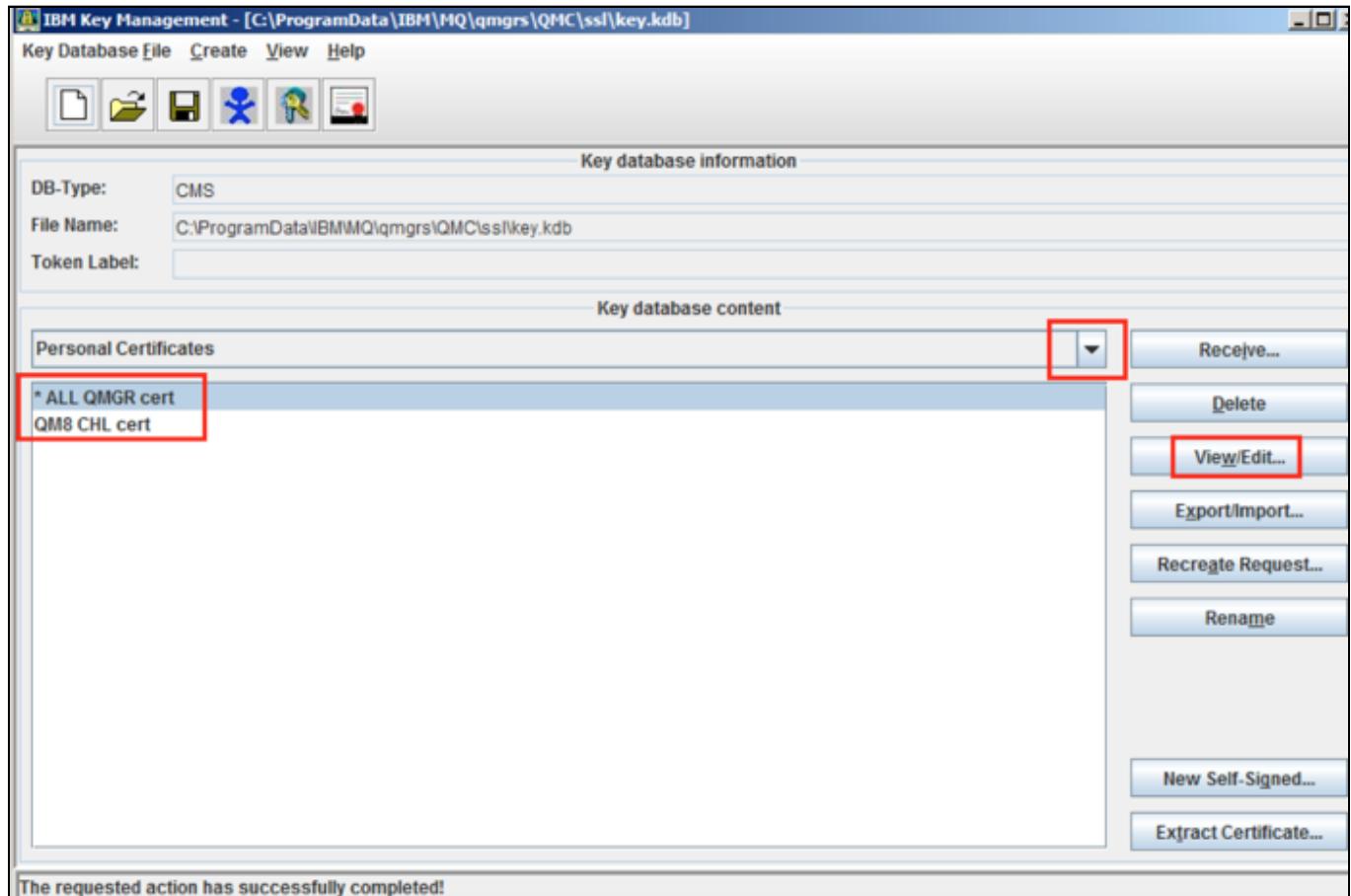
9. Select OK.



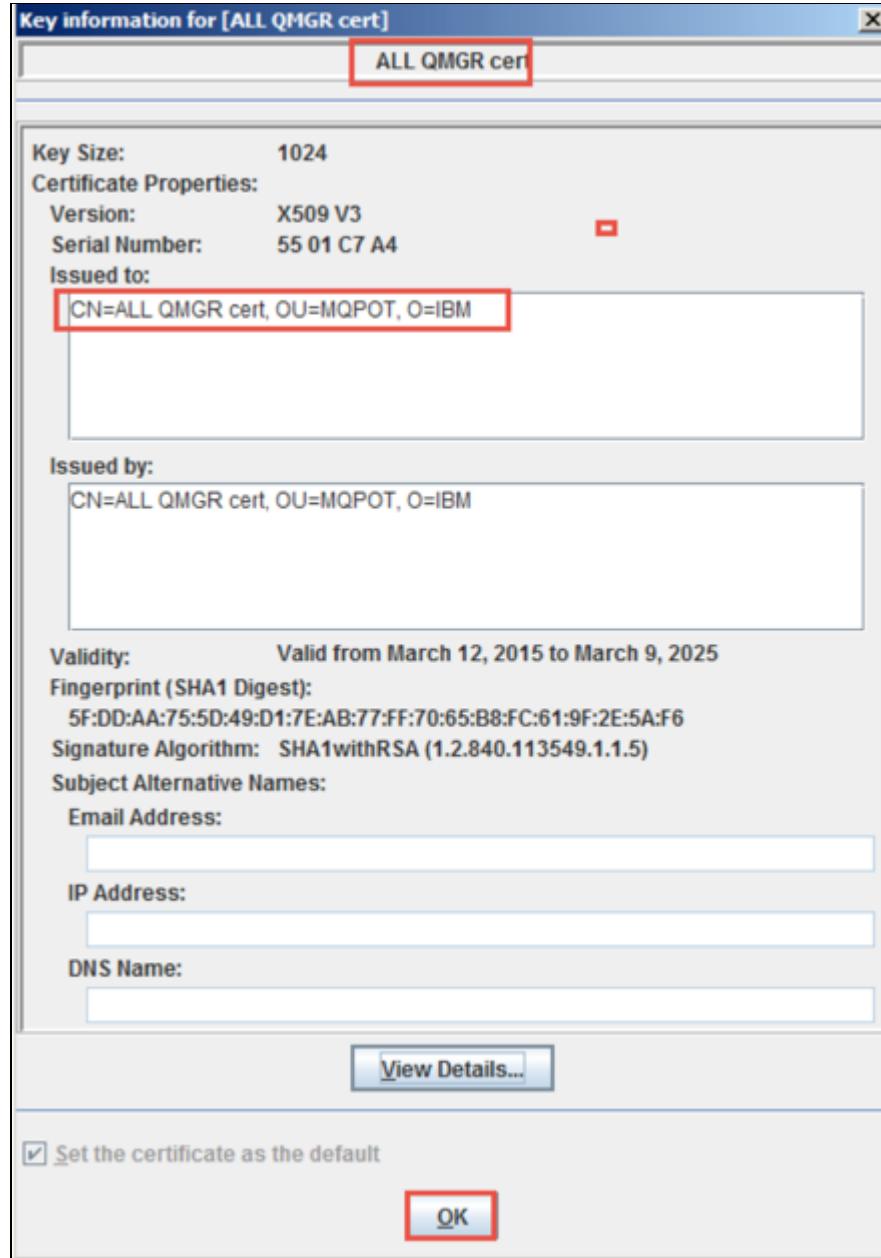
10. Enter the password which is **password** when prompted and click OK.



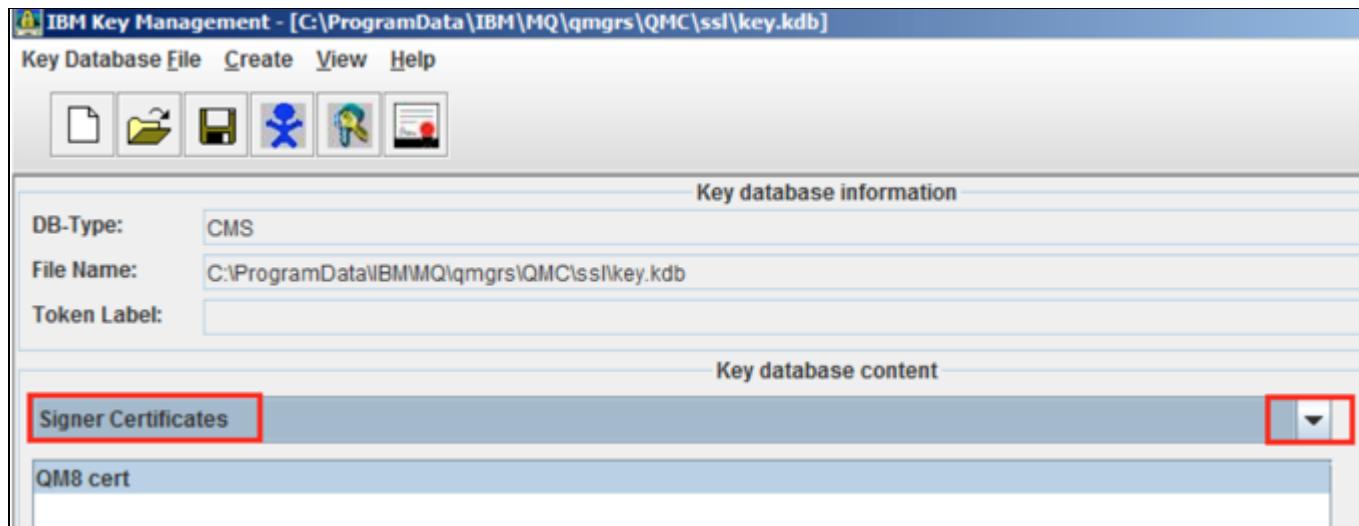
11. When Ikeyman opens, the personal certificates are displayed. You will see the installed certificate names listed. To review the content of a certificate you can select a certificate in the list and select 'view/edit'.



12. Select 'ALL QMGR cert' and click View/Edit.

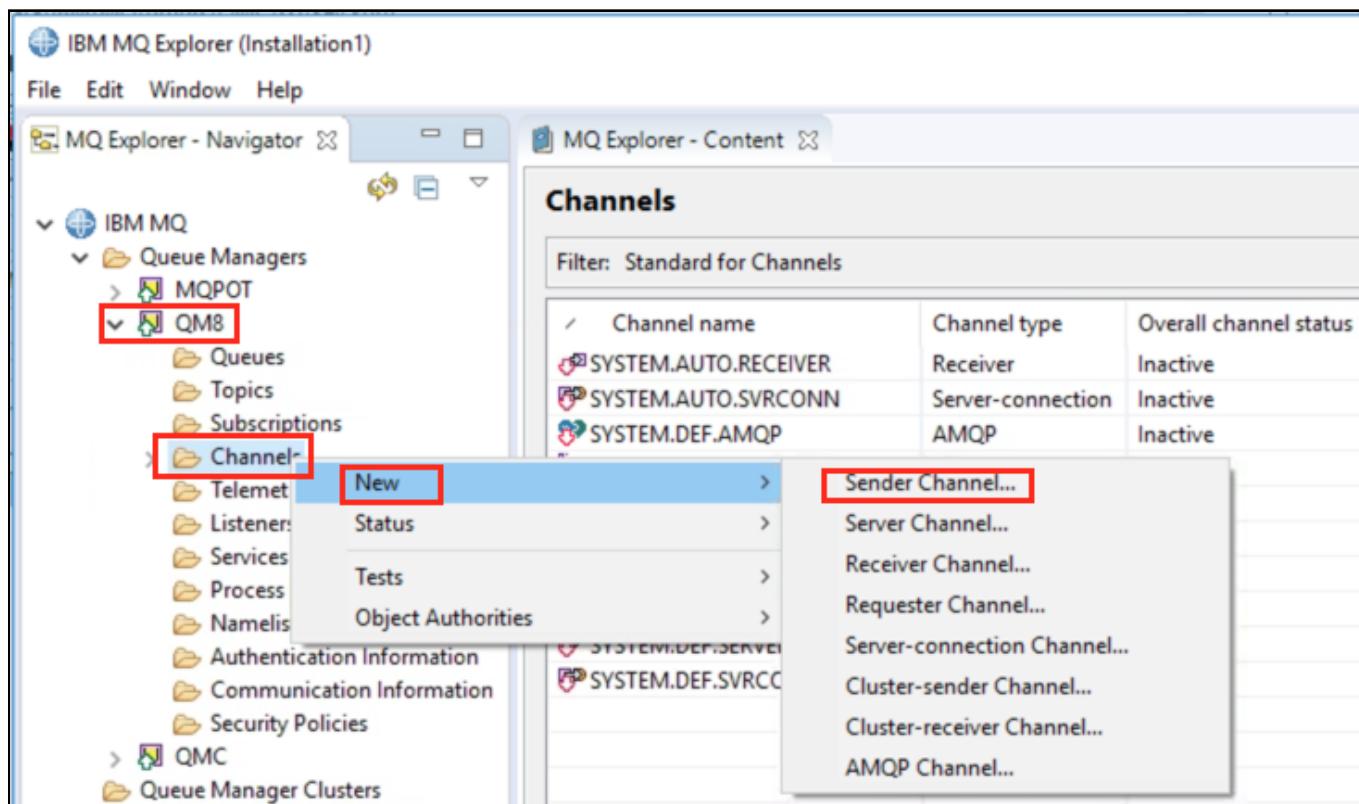


13. If you want to review signer certificates you can use the pull down button.

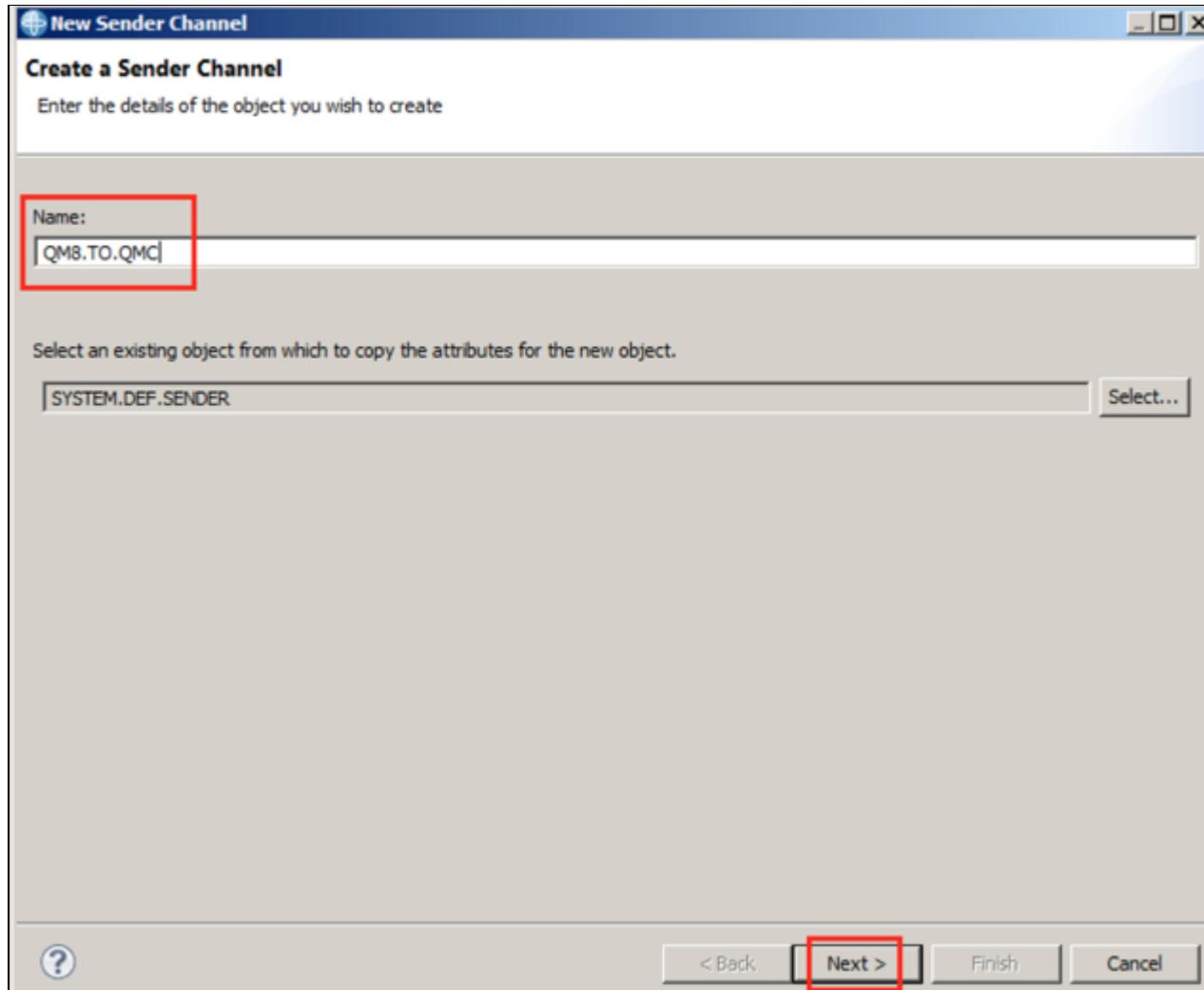


On QM8 define the SDR channel QM8.TO.QMC

1. From the MQ Explorer, under QM8, right click channels, > New > Sender channel.

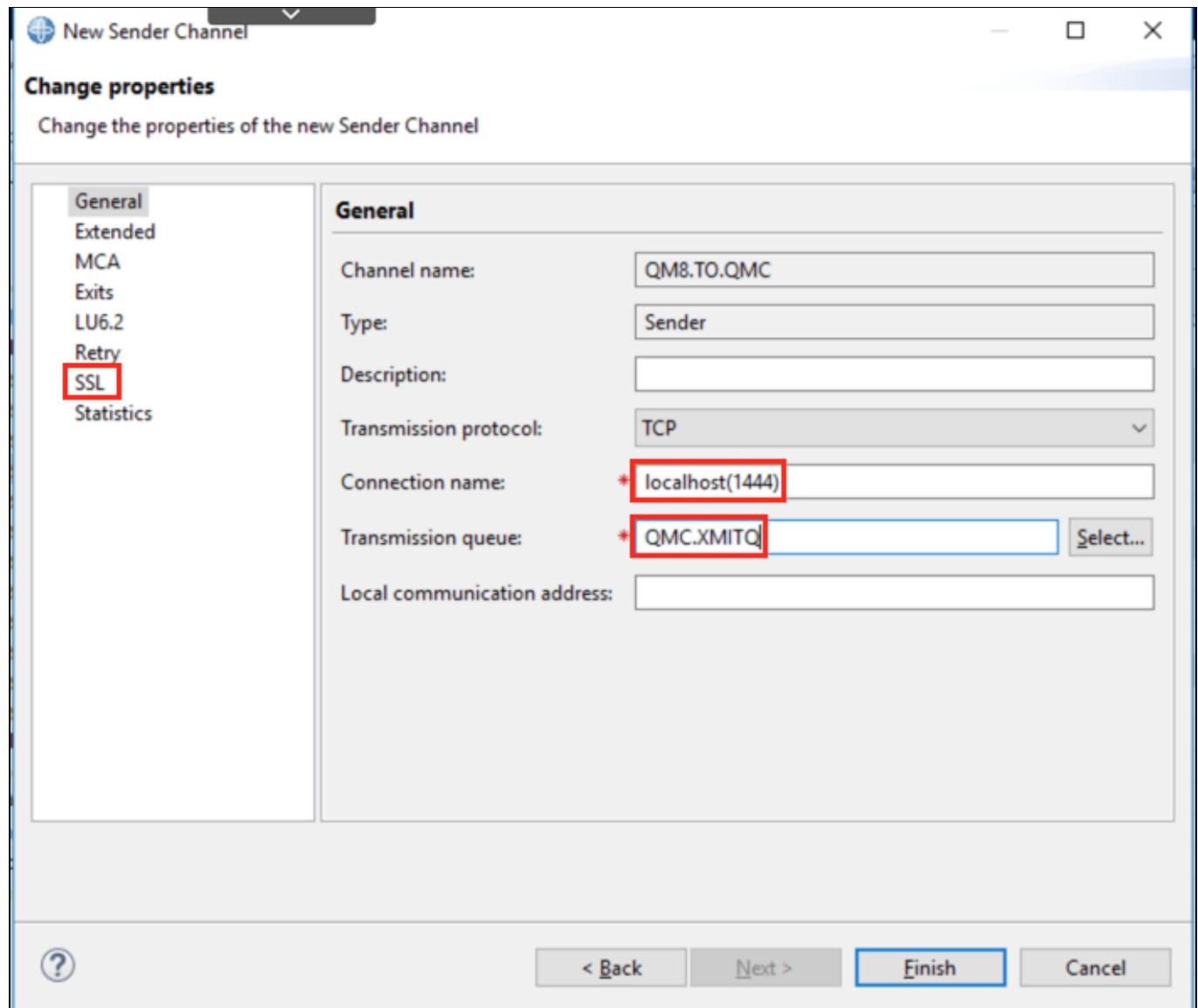


2. On the next panel, enter the channel name 'QM8.TO.QMC' and click Next.

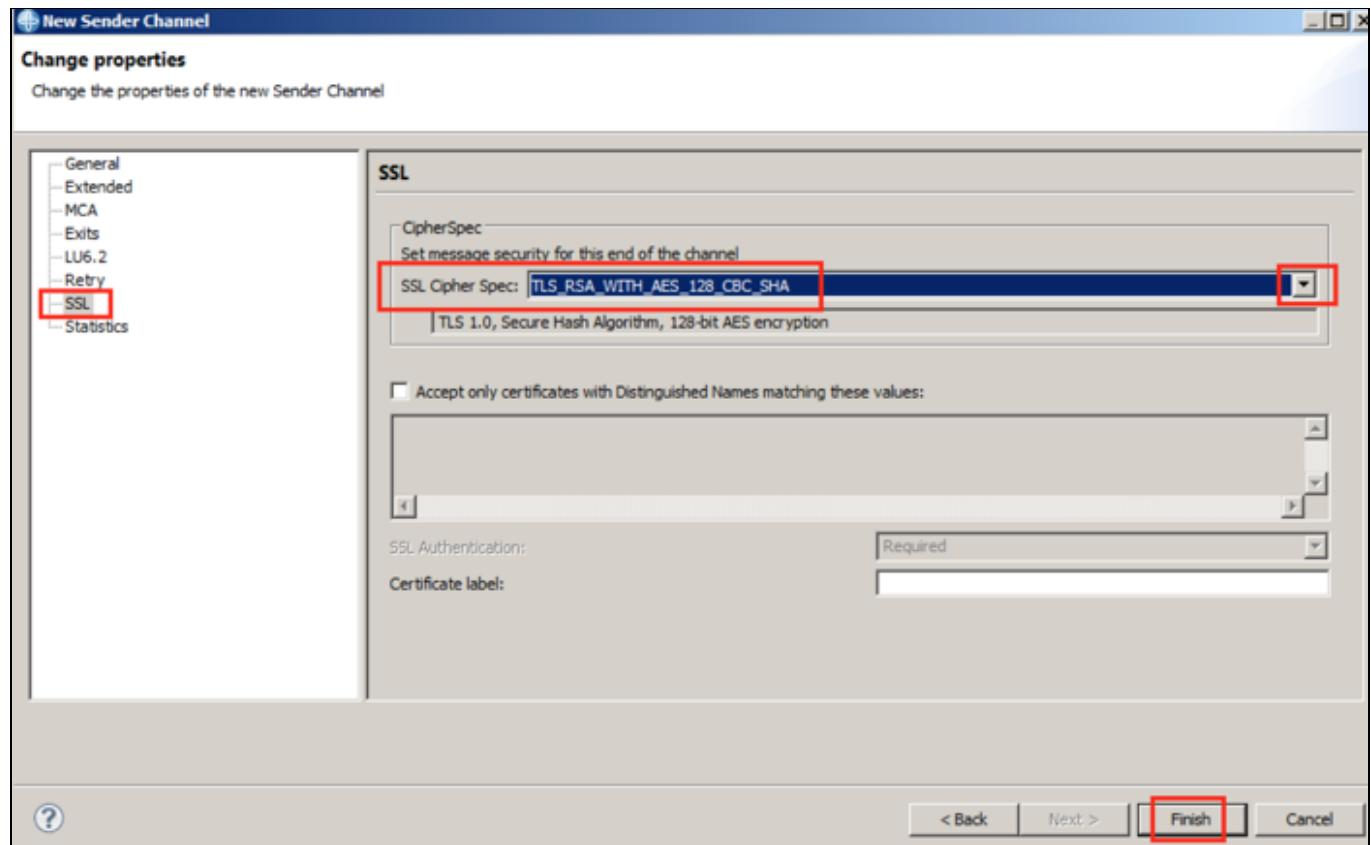


3. Specify the properties below:

Property	Value
Connection Name	localhost(1444)
Transmission queue	QMC.XMITQ



4. Select the 'SSL' from the Properties list on the left.
5. Use the pull down tab to select the SSL Cipher Spec and choose:
SSL Cipher Spec: **TLS_RSA_WITH_AES_128_CBC_SHA**
6. Click finish.



In this example we have left the Certificate label (CERTLBL) blank for this channel, therefore the certificate to be sent to the remote end will be QM8 *queue manager* **CERTLBL** property. We set this to 'QM8 CHL cert' when we configured the SSL properties on QM8.

7. Click OK to dismiss the results pane.



Channel 'QM8.TO.QMC' now appears in the channel list.

The screenshot shows the IBM MQ Explorer interface. On the left, the Navigator pane displays a tree structure under 'IBM MQ' with 'Queue Managers' expanded, showing 'MQPOT' and 'QM8'. Under 'QM8', 'Channels' is selected. The Content pane is titled 'Channels' and lists several entries:

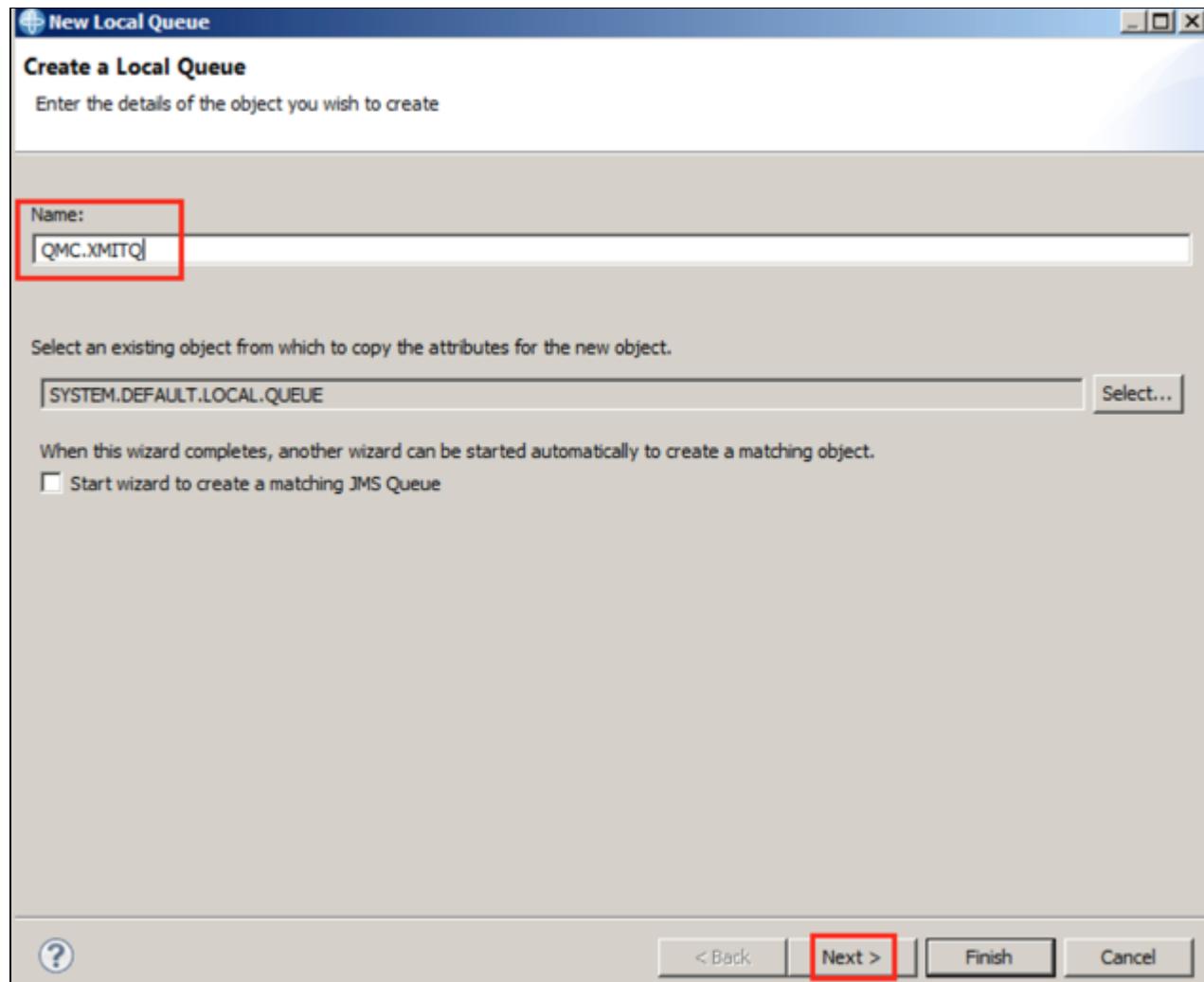
Channel name	Channel type	Overall channel status	Conn name	Transmission queue
QM8.TO.QMC	Sender	Inactive	localhost(1444)	QMC.XMITQ
SYSTEM.AUTO.RECEIVER	Receiver	Inactive		
SYSTEM.AUTO.SVRCONN	Server-connection	Inactive		
SYSTEM.DEF.AMQP	AMQP	Inactive		
SYSTEM.DEF.CLUSRCVR	Cluster-receiver	Inactive		
SYSTEM.DEF.CLUSSDR	Cluster-sender	Inactive		
SYSTEM.DEF.RECEIVER	Receiver	Inactive		
SYSTEM.DEF.REQUESTER	Requester	Inactive		

8. You also need to define the transmission queue QMC.XMITQ. In MQ Explorer, under QM8 right-click Queues and select New > Local Queue.

The screenshot shows the IBM MQ Explorer interface. The Navigator pane shows 'IBM MQ' with 'QM8' selected. A context menu is open over 'Queues', with 'New' highlighted. A sub-menu is displayed with 'Local Queue...' selected. The Content pane is titled 'Queues' and lists existing queues:

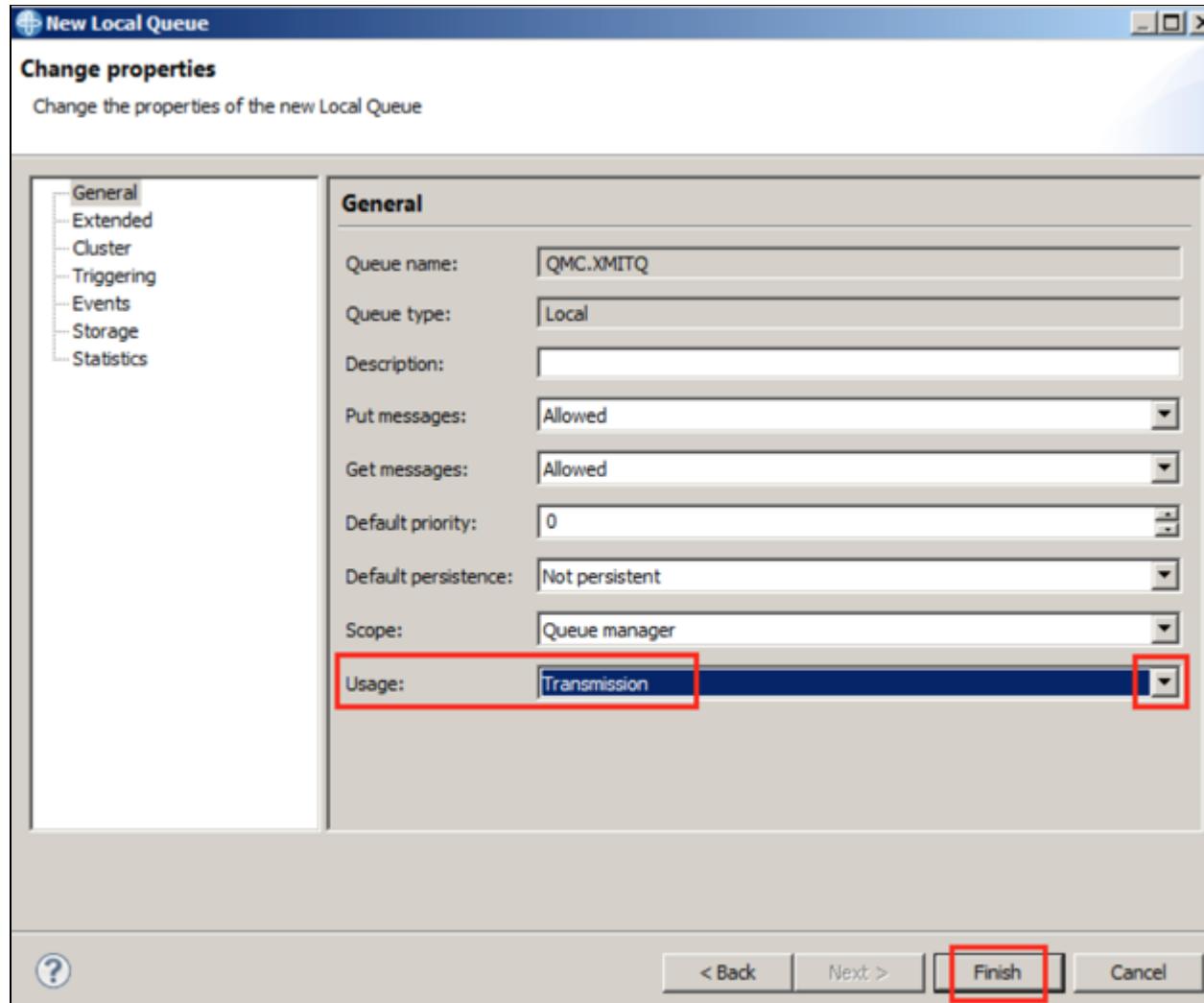
Queue name	Queue type
IN.CONFIG.EVENT	Local
IN.LOGGER.EVENT	Local
SYSTEM.ADMIN.PERFM.EVENT	Local
SYSTEM.ADMIN.PUBSUB.EVENT	Local
SYSTEM.ADMIN.QMGR.EVENT	Local
SYSTEM.ADMIN.STATISTICS.QUEUE	Local

9. Enter Queue name **QMC.XMITQ** in the Name field and select Next.

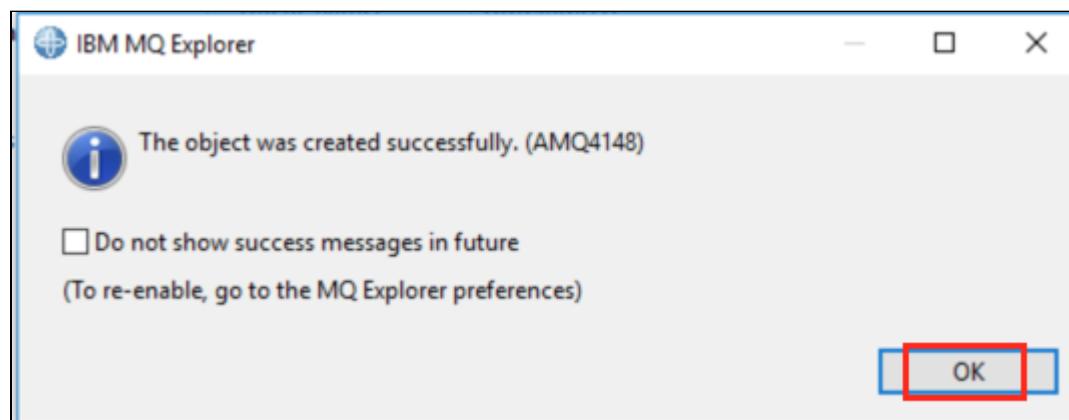


10. Alter the Usage field to ‘Transmission’.

11. Click Finish.



12. Click OK to dismiss the results pane.



13. The new transmission queue QMC.XMITQ will appear in the Queues list.

The screenshot shows the 'IBM MQ Explorer (Installation1)' interface. In the left pane, under 'IBM MQ > Queue Managers > QM8 > Queues', the queue 'QMC.XMITQ' is listed. This queue is highlighted with a red box. The right pane displays a table titled 'Queues' with one row for 'QMC.XMITQ'. The columns are 'Queue name' (QMC.XMITQ), 'Queue type' (Local), 'Open input count' (0), 'Open output count' (0), and 'Current queue depth' (0).

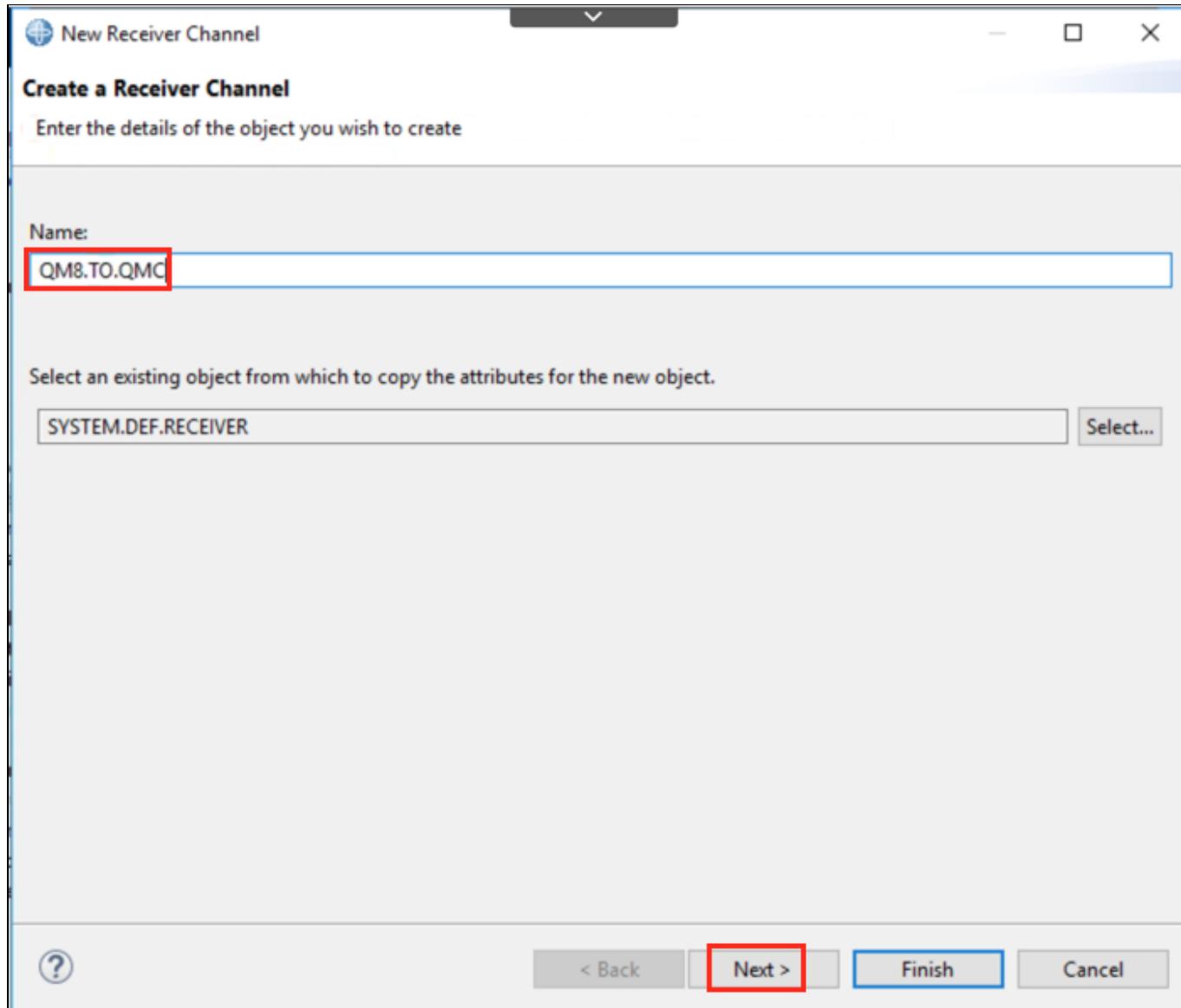
On QMC define the RCVR channel

1. In the MQ Explorer under QMC, right-click Channels and select New > Receiver channel.

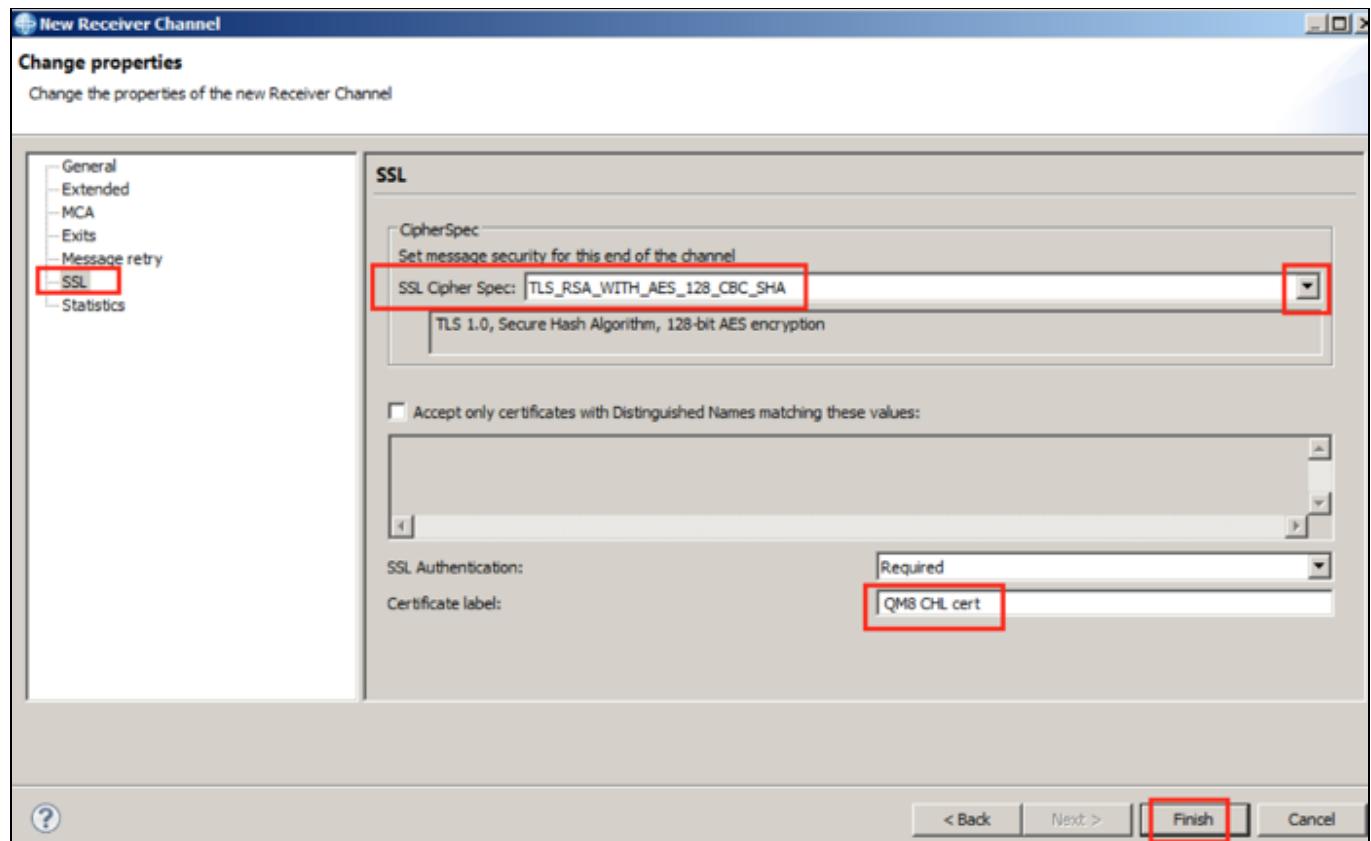
The screenshot shows the 'MQ Explorer - Navigator' and 'MQ Explorer - Content' panes. In the Navigator pane, the tree structure includes 'IBM WebSphere MQ > Queue Managers > QM8 > QMC > Channels'. A context menu is open over the 'Channels' node, with the 'New' option highlighted. A sub-menu titled 'Scheme: Standard for Channels - Distributed' appears, containing options like 'Sender Channel...', 'Server Channel...', 'Receiver Channel...', 'Requester Channel...', 'Server-connection Channel...', 'Cluster-sender Channel...', and 'Cluster-receiver Channel...'. The 'Receiver Channel...' option is also highlighted with a red box.

2. Enter channel name 'QM8.TO.QMC'.

3. Click Next.



4. Select the 'SSL' from the Properties list on the left.
5. Use the pull down tab to select the SSL Cipher Spec and choose:
SSL Cipher Spec: **TLS_RSA_WITH_AES_128_CBC_SHA**
Certificate label: **'QM8 CHL cert'**
6. Click finish.



7. Click OK to dismiss the results pane.



8. The receiver channel QM8.TO.QMC now appears in queue manager QMC Channels list.

The screenshot shows the IBM MQ Explorer interface. On the left, the Navigator pane displays a tree structure under 'IBM MQ' for 'QM8'. A red box highlights the 'QM8' node. Under 'QM8', the 'Channels' node is also highlighted with a red box. On the right, the Content pane is titled 'Channels' and contains a table with one row. The table has columns for 'Channel name', 'Channel type', and 'Overall channel status'. The single entry is 'QM8.TO.QMC', 'Receiver', and 'Inactive' respectively. A red box highlights the entire row.

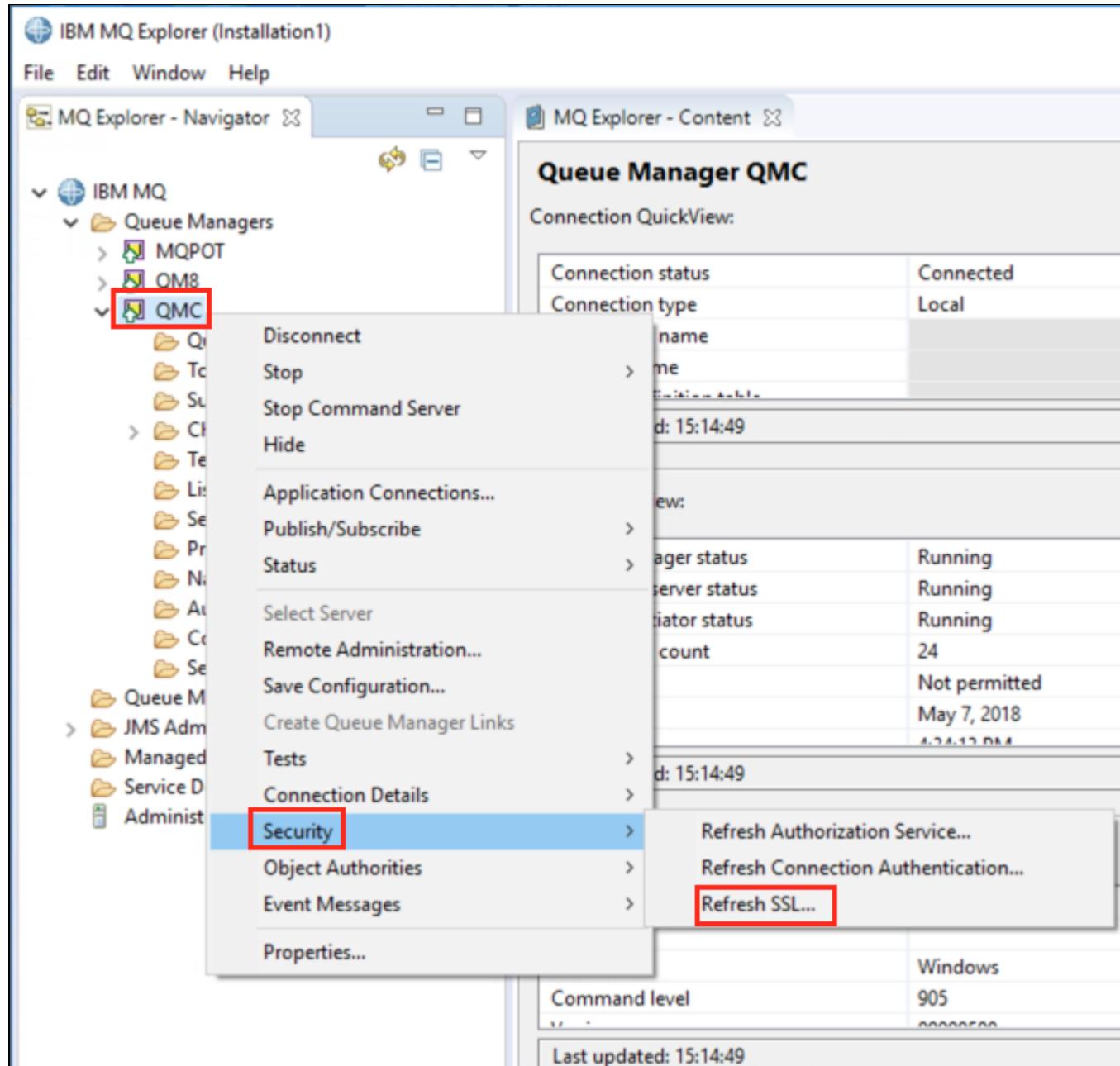
Channel name	Channel type	Overall channel status
QM8.TO.QMC	Receiver	Inactive

Alternatively, you could issue the following commands from a runmqsc command prompt:

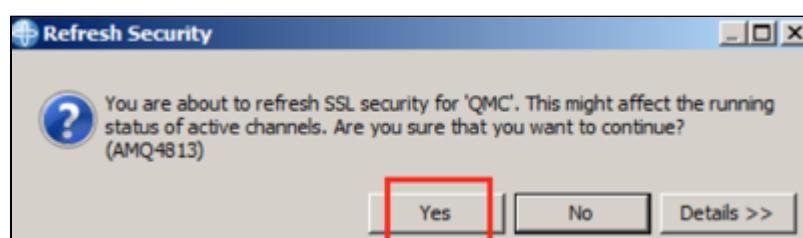
```
ALTER CHL(QM8.TO.QMC) SSLCIPH(TLS_RSA_WITH_AES_128_CBC_SHA) CERTLBL('QM8 CHL cert')
```

Setting the receiver channel certificate label as 'QM8 CHL cert' overrides the queue manager property CERTLBL for QMC ('ALL QMGR cert').

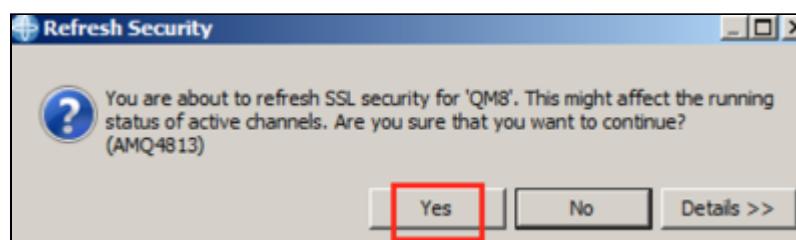
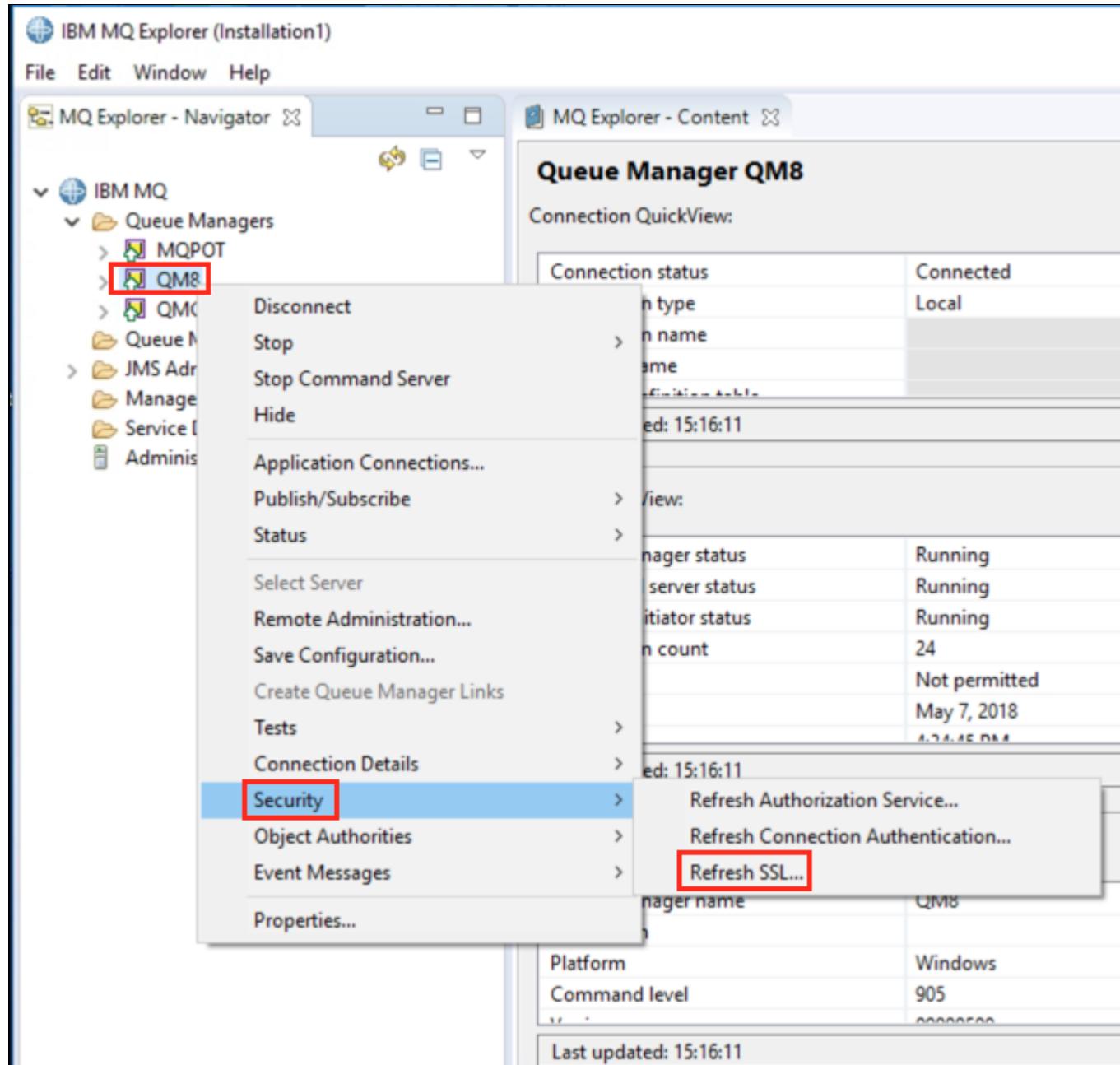
9. Refresh security for both queue managers to ensure we pick up all security changes.
10. This can be done from the MQ Explorer. Right-click the queue manager QMC, and select Security > Refresh SSL.



11. Click Yes to confirm the refresh.



12. Repeat Step 10 – 11 for queue manager QM8.



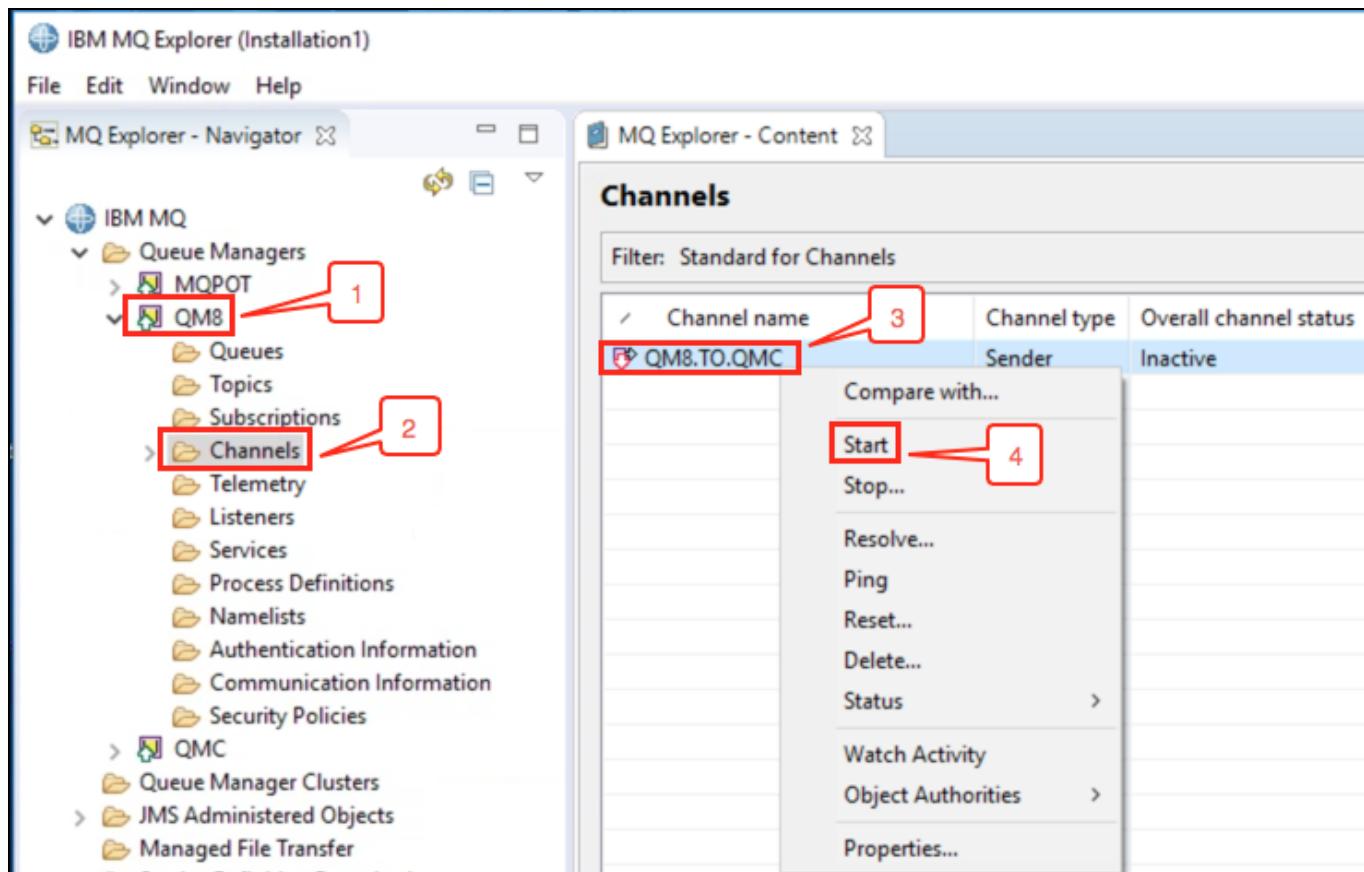
Alternatively, you could refresh security using the runmqsc command prompt by issuing the following command:

```
REFRESH SECURITY(*) TYPE(SSL)
```

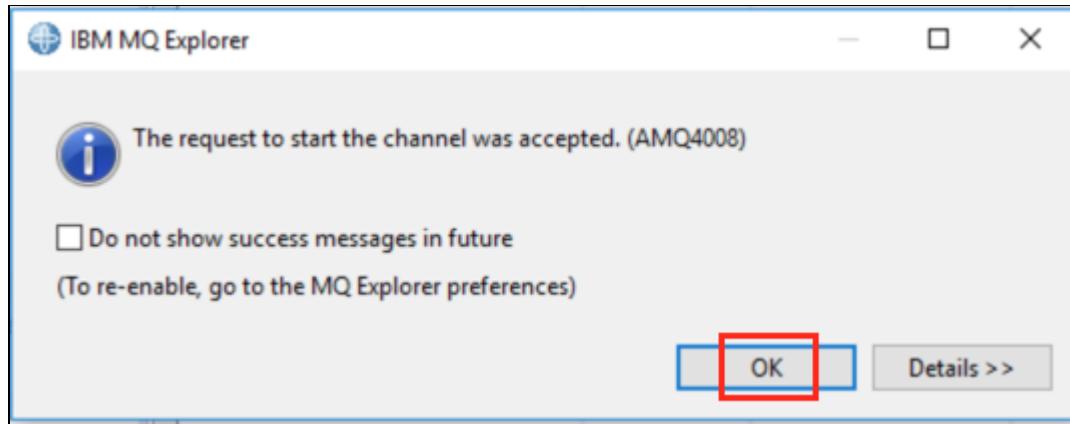
1 Note:

When the Refresh SSL operation is performed, all running SSL channels are stopped and restarted. However MQ Explorer will only wait 30 seconds, so if your channels take longer to refresh then you will see error message AMQ4562. The refresh will continue and channels will be restarted after the refresh completes. In case your channels do not restart, you should check the MQ error logs for messages.

13. Now start the channel from the MQ Explorer. Under QM8 select Channels. Right-click channel QM8.TO.QMC and select Start.



14. Click OK to dismiss the results pane.



Alternately you could issue the following runmqsc command:

START CHL(QM8.TO.QMC)

The channel should go to 'running' status.

A screenshot of the IBM MQ Explorer application window. The left pane shows the Navigator with nodes like IBM MQ, Queue Managers (QM01, QM8), and Channels. The Channels node under QM8 is highlighted with a red box. The right pane shows the Content view with a table titled "Channels".

Channel name	Channel type	Overall channel status	Conn name	Transmission queue
QM8.TO.QMC	Sender	Running	localhost(1444)	QMC.XMITQ

15. Check the channel status. From a command prompt enter:

runmqsc QMC

DIS CHS(QM8.TO.QMC) SSLPEER SSLCERTI

```
Command Prompt - runmqsc QMC

C:\Users\ibmdemo.DESKTOP-6DSOOH2>runmqsc QMC
5724-H72 (C) Copyright IBM Corp. 1994, 2018.
Starting MQSC for queue manager QMC.

DIS CHS(QM8.TO.QMC) SSLPEER SSLCERTI
  1 : DIS CHS(QM8.TO.QMC) SSLPEER SSLCERTI
AMQ8417I: Display Channel Status details.
  CHANNEL(QM8.TO.QMC)                      CHLTYPE(RCVR)
  CONNAME(127.0.0.1)                        CURRENT
  RQMNAME(QM8)
  SSLCERTI(CN=QM8 CHL cert,OU=MQPOT,O=IBM)
  SSLPEER(SERIALNUMBER=54:DC:A7:E0,CN=QM8 CHL cert,OU=MQPOT,O=IBM)
  STATUS(RUNNING)                           SUBSTATE(RECEIVE)
```

16. Look at the SSLPEER and SSLCERTI fields on the receiver side. SSLCERTI shows what the 'remote' side is using - in this case 'QM8 CHL cert' is being used. This was specified in the QM8 queue manager CERTLBL property and is used because the sender channel CERTLBL field was blank.
17. End the runmqsc command prompt and start it for QM8. Issue the same channel status command for QM8.

Now look at the SSLPEER and SSLCERTI information on the sender side of the channel. It shows 'QM8 CHL cert' is being used by the remote side. We specified this on the receiver channel definition in the CERTLBL property, and this overrides the certificate specified in the queue managers CERTLBL property.

```
Command Prompt

C:\Users\ibmdemo.DESKTOP-6DSOOH2>runmqsc QM8
5724-H72 (C) Copyright IBM Corp. 1994, 2018.
Starting MQSC for queue manager QM8.

DIS CHS(QM8.TO.QMC) SSLPEER SSLCERTI
  1 : DIS CHS(QM8.TO.QMC) SSLPEER SSLCERTI
AMQ8417I: Display Channel Status details.
  CHANNEL(QM8.TO.QMC)                      CHLTYPE(SDR)
  CONNAME(127.0.0.1(1444))                CURRENT
  RQMNAME(QMC)
  SSLCERTI(CN=QM8 CHL cert,OU=MQPOT,O=IBM)
  SSLPEER(SERIALNUMBER=54:DC:A7:E0,CN=QM8 CHL cert,OU=MQPOT,O=IBM)
  STATUS(RUNNING)                           SUBSTATE(MQGET)
  XMITQ(QMC.XMITQ)
```

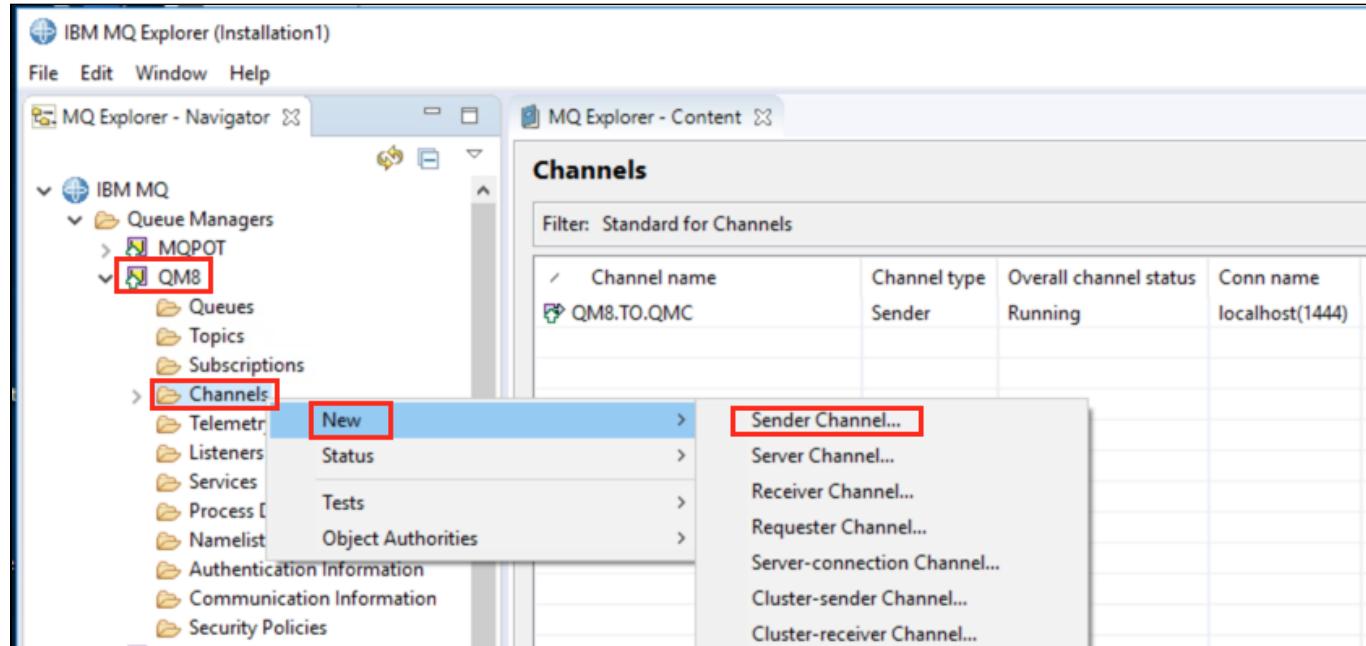
Create a new SDR RCVR channel using the certificate in the receivers queue manager property CERTLBL

If we create a second channel leaving the CERTLBL blank on the RCVR channel definition this should use the certificate specified in the queue manager property CERTLBL.

If you need help defining a new channel, refer to section “On QM8 define the SDR channel QM8.TO.QMC” Steps 1 – 13 to refresh your memory.

1. On QM8 create new SDR channel QM8.TO.QMC.CHL2 using the MQ Explorer as in previous steps specifying the SSL cipher TLS_RSA_WITH_AES_128_CBC_SHA. Specify a different transmission queue name QMC.XMITQ.CHL2.

Use the following screen-shots as a guide.



New Sender Channel

Create a Sender Channel

Enter the details of the object you wish to create

Name:

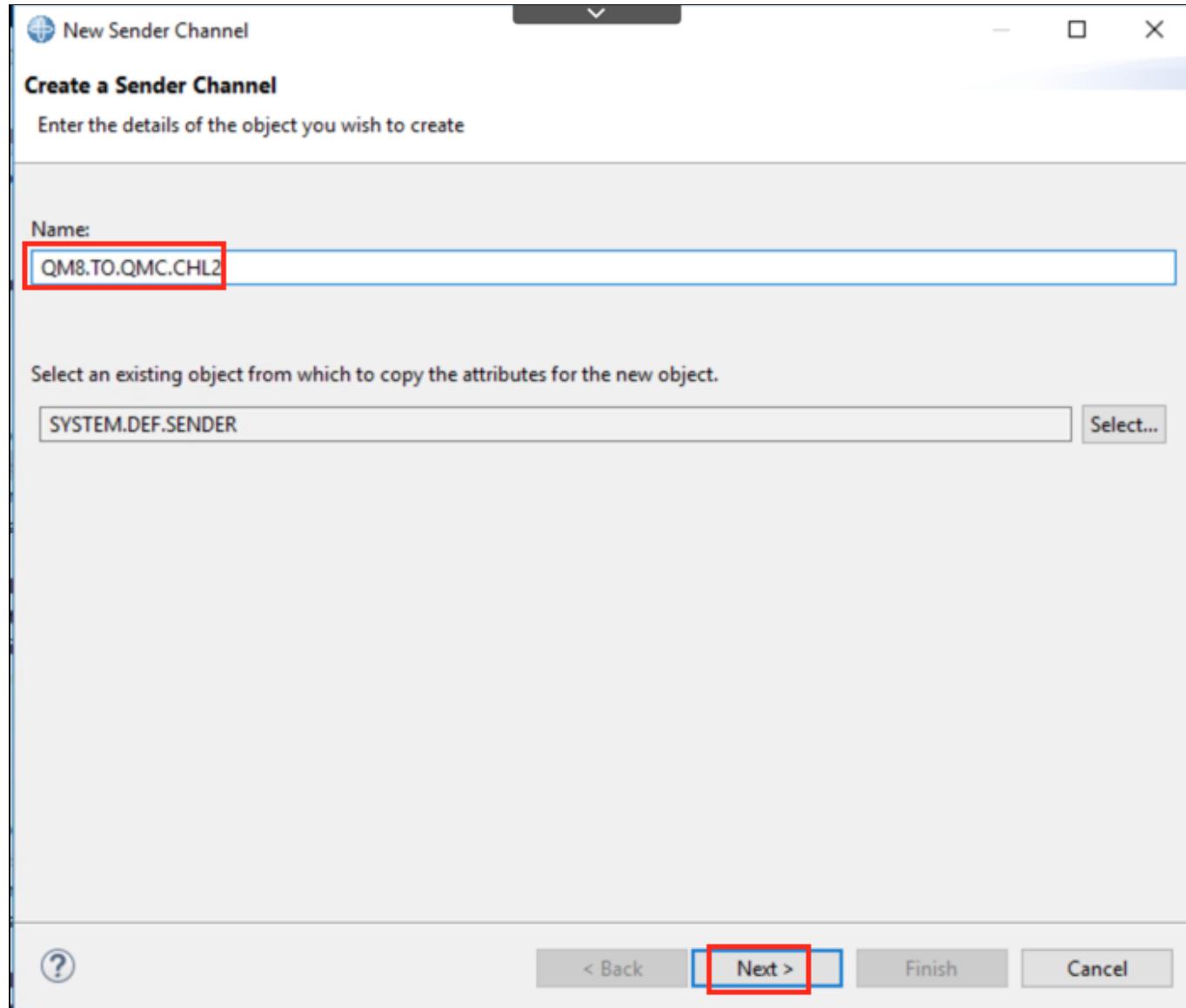
QM8.TO.QMC.CHL2

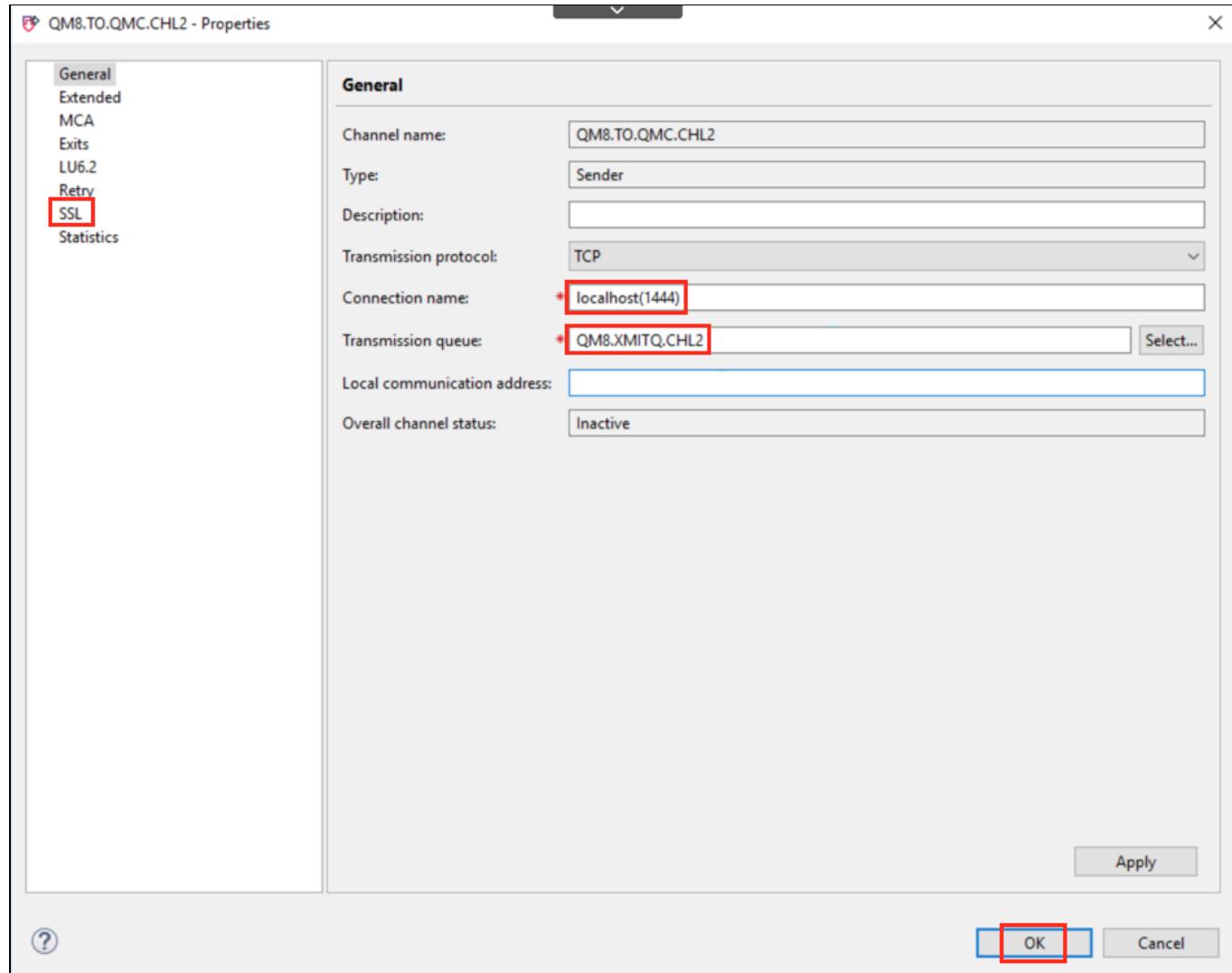
Select an existing object from which to copy the attributes for the new object.

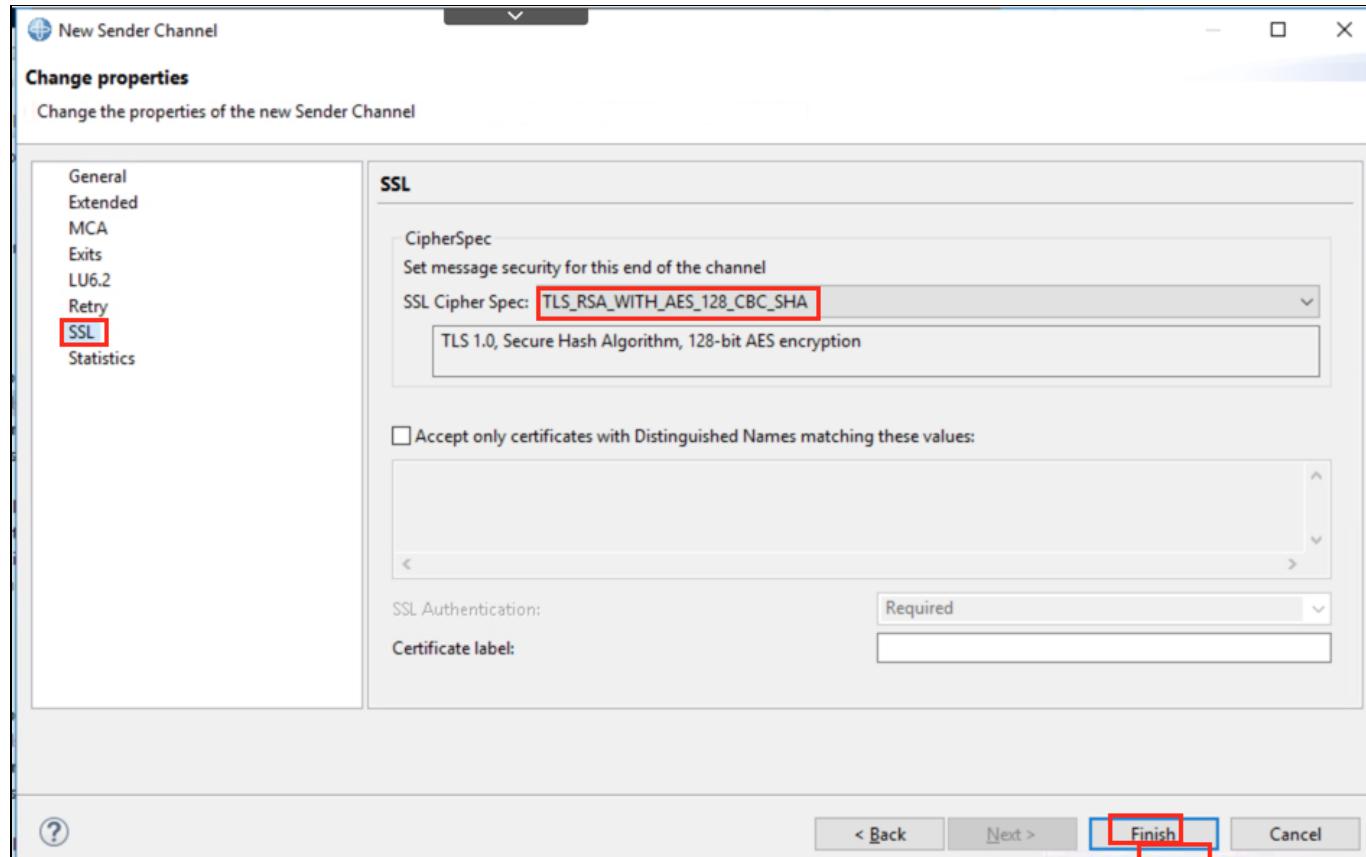
SYSTEM.DEF.SENDER Select...

?

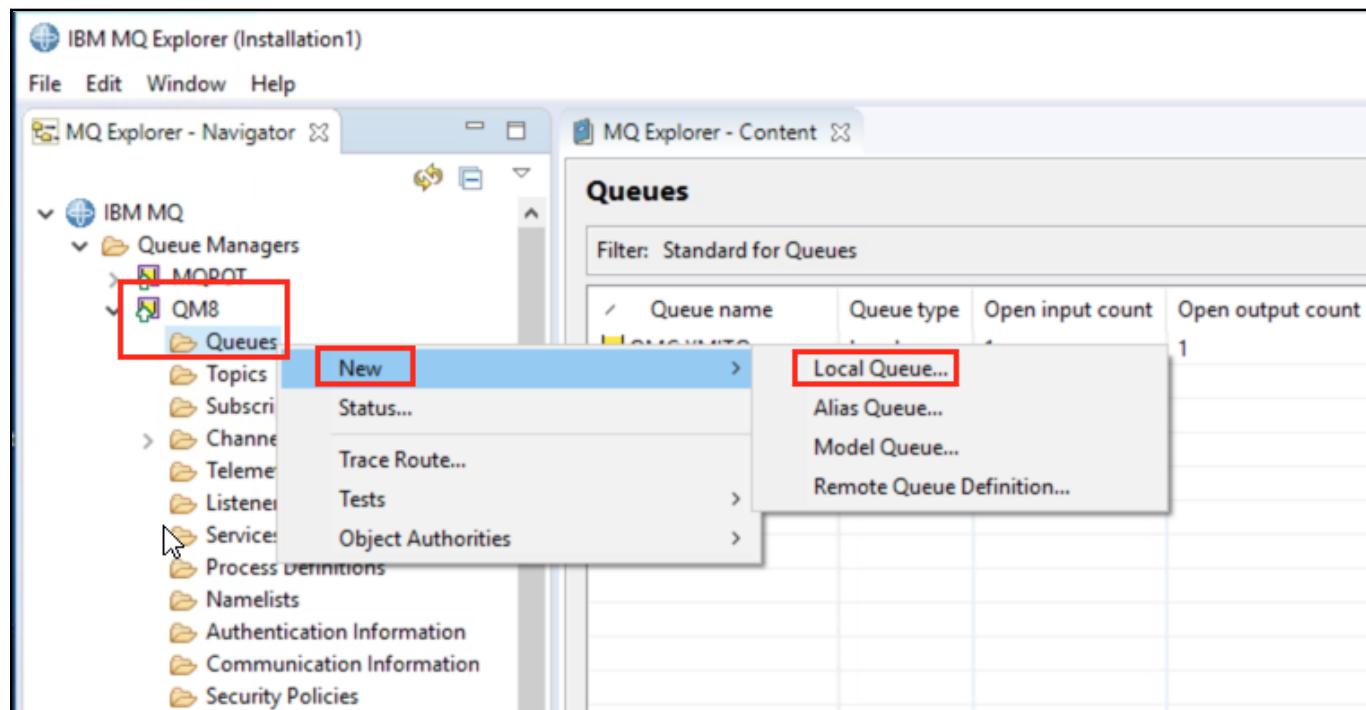
< Back Next > Finish Cancel

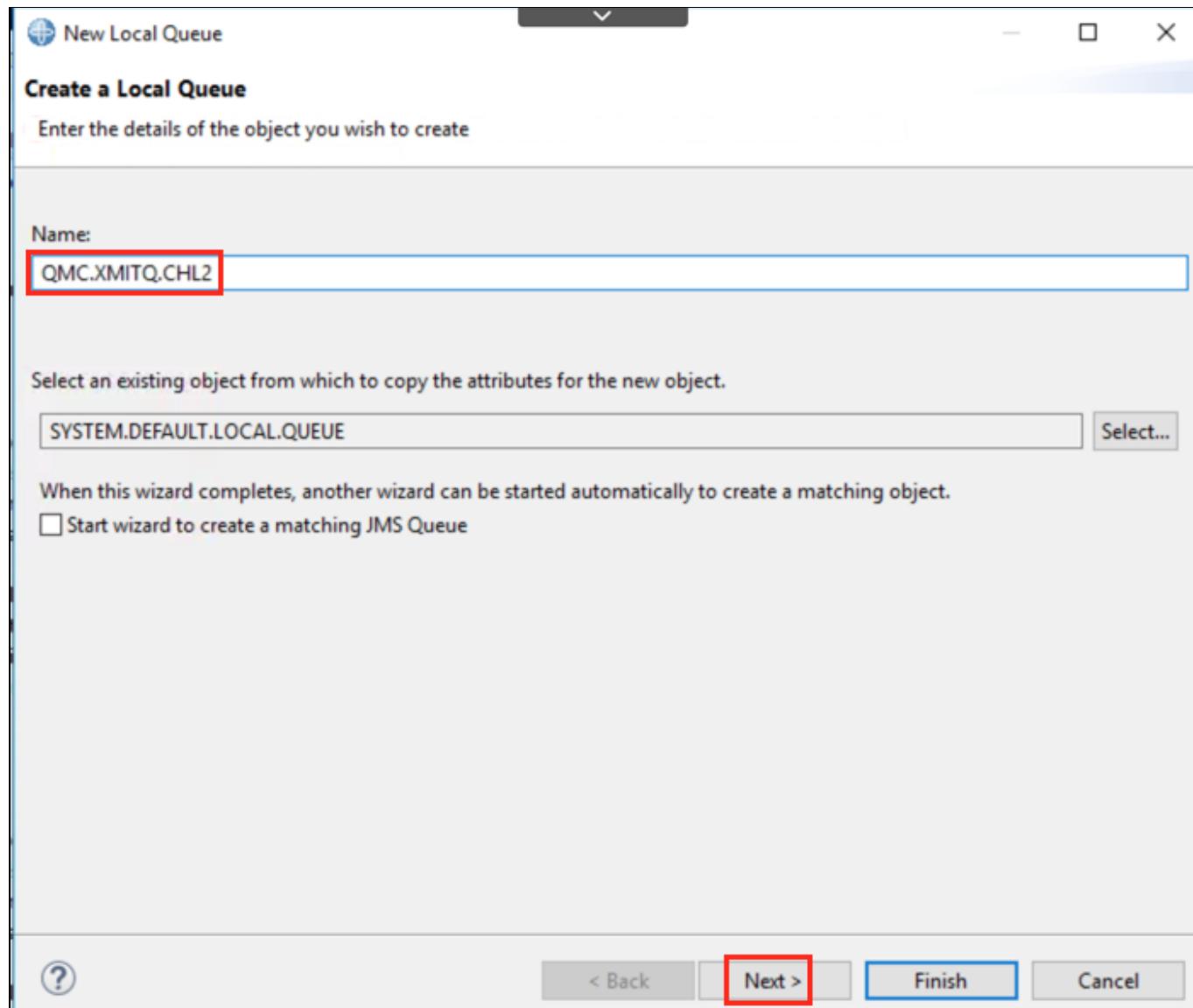


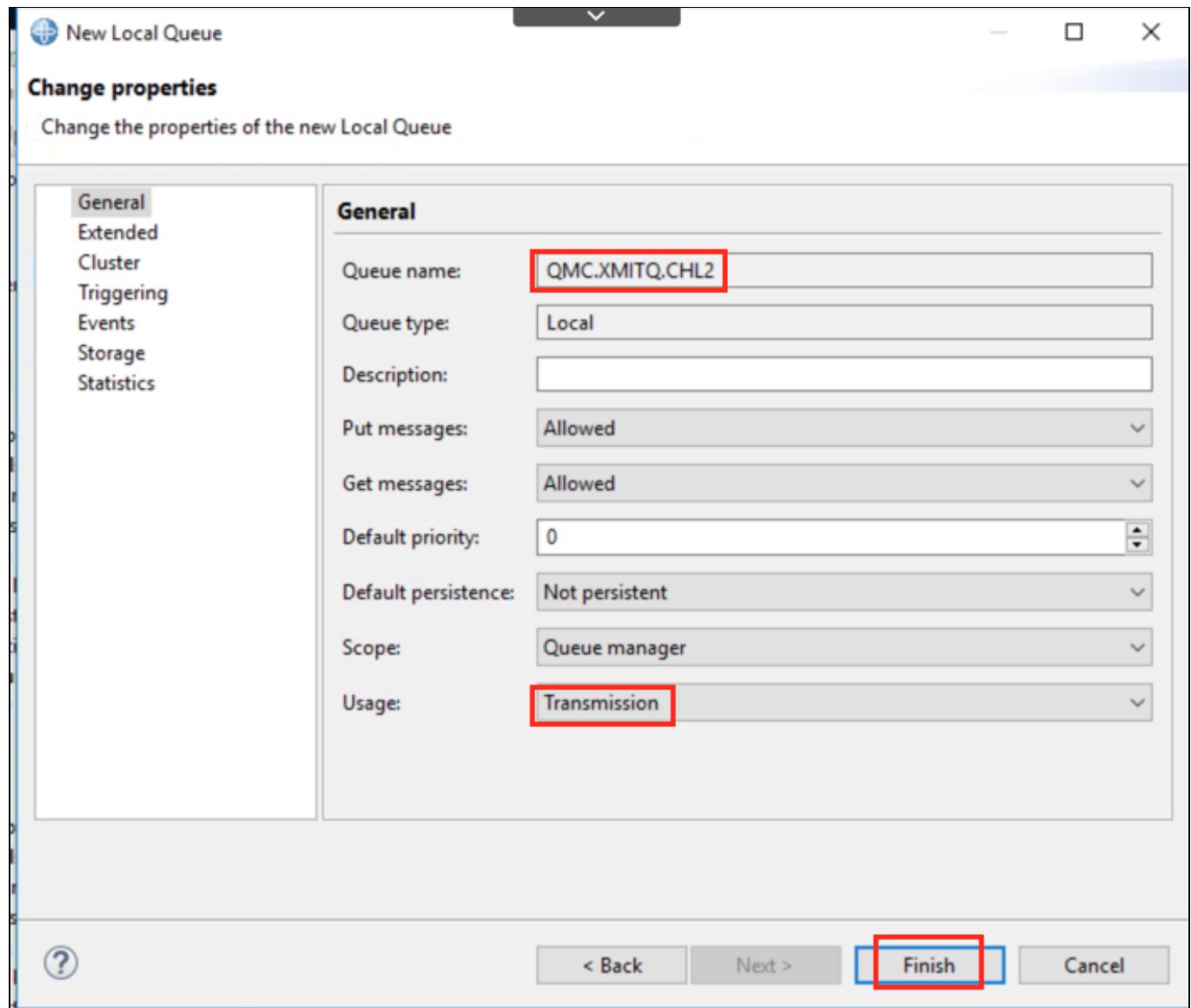




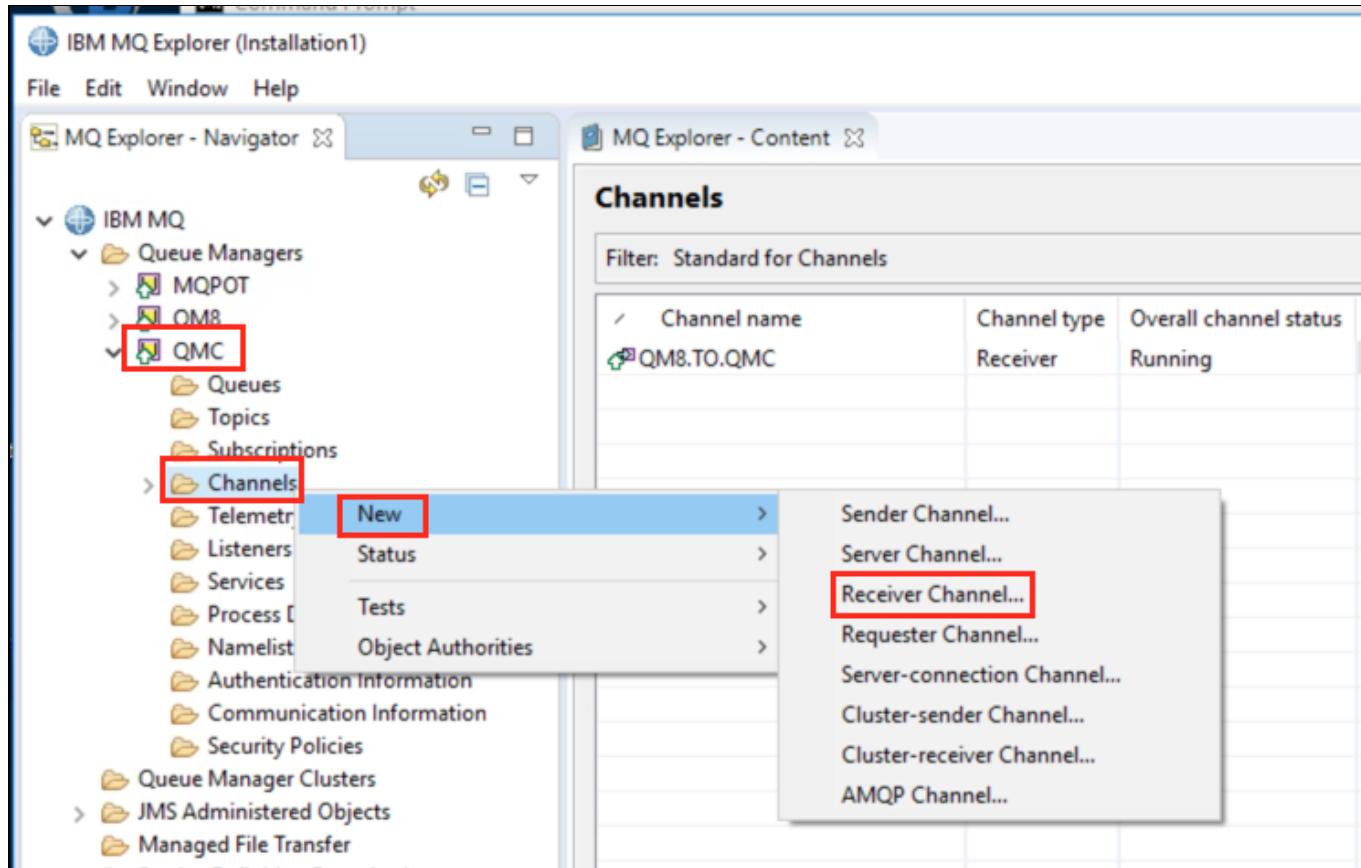
2. Create Local Queue QMC.XMITQ.CHL2 and specify Transmission in the Usage field.

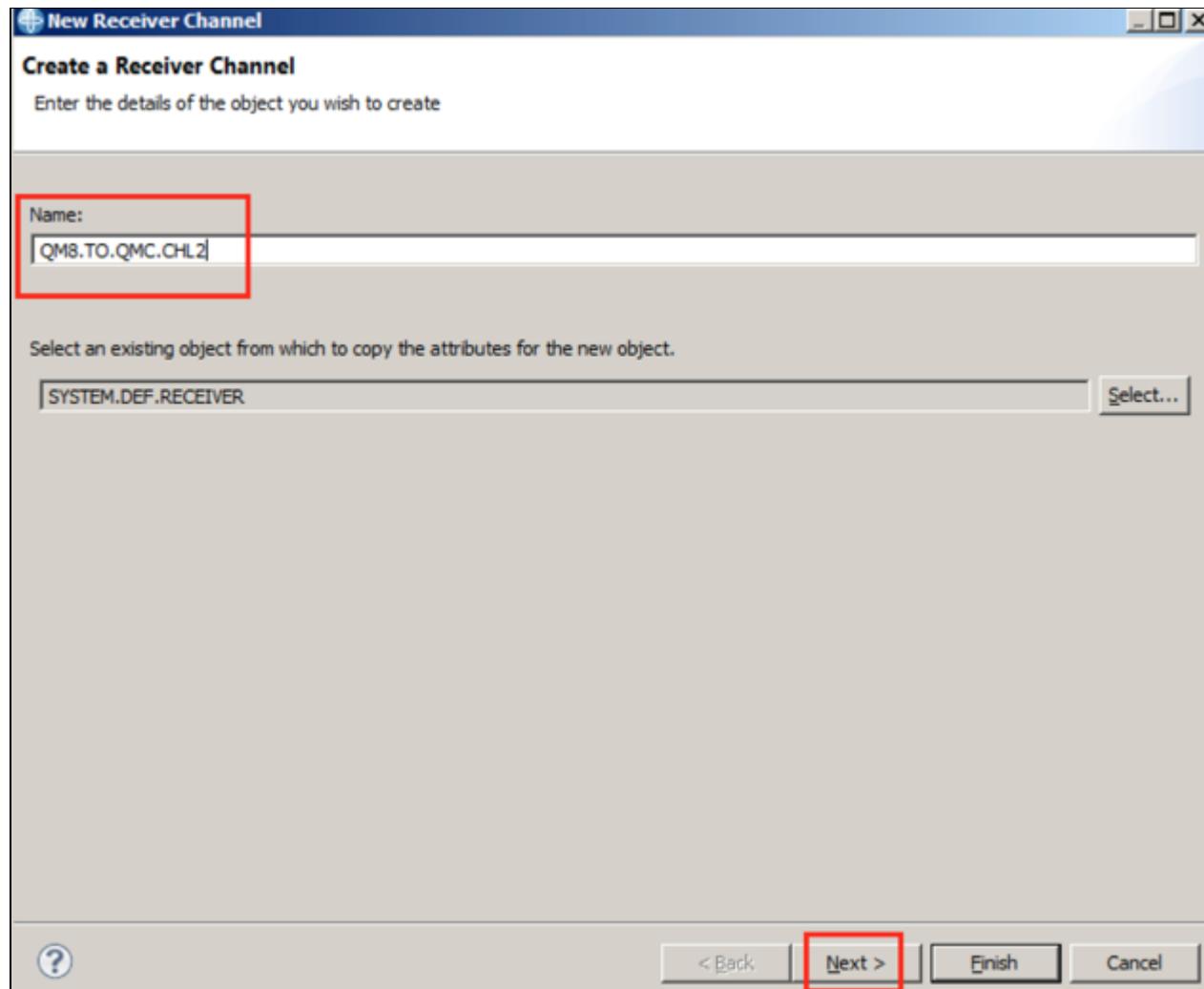


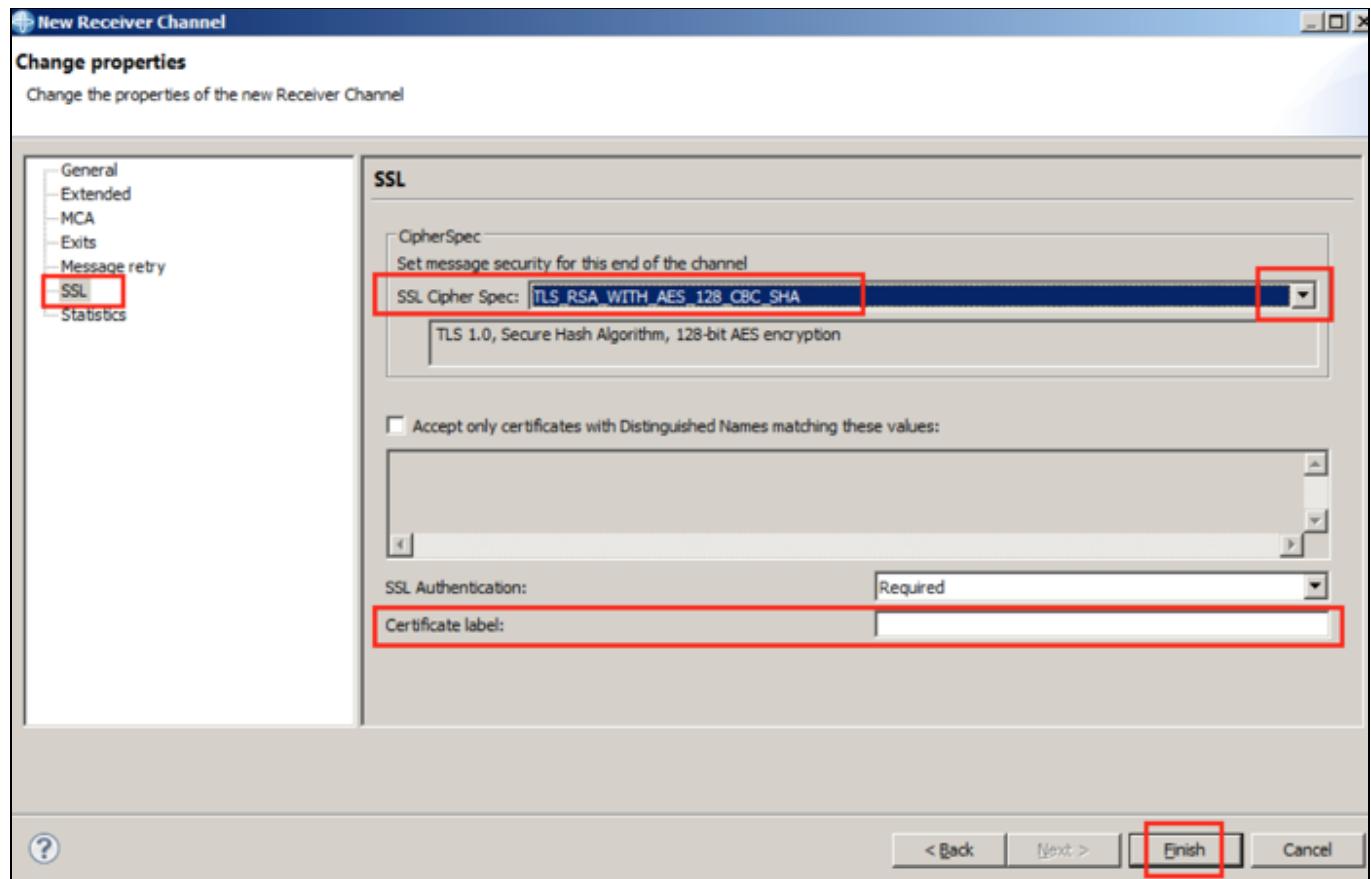




3. On QMC create new RCVR channel QM8.TO.QMC.CHL2 and leave the CERTLBL blank on the RCVR definition so this time the channel will be using the QMC queue manager SSL property CERTLBL.

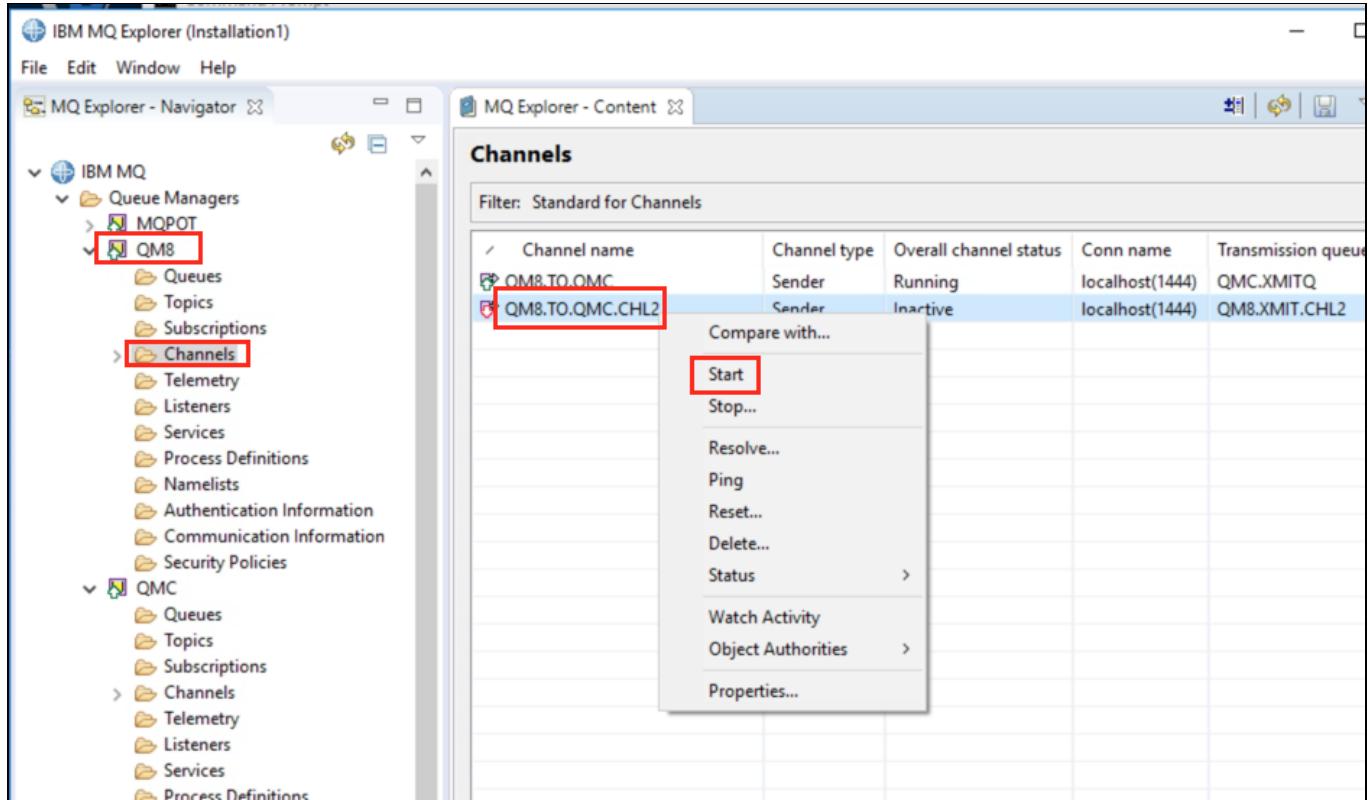






At this point there is no need to refresh security because none of the queue manager's SSL attributes have changed and nothing in the key repository has been changed.

4. From QM8, start channel QM8.TO.QMC.CHL2.



Note:

Note that if you do have any problems starting the channel you should check the queue manager error logs at both ends of the channel. If you do need to make any changes to the queue manager SSL attributes then a REFRESH SECURITY TYPE(SSL) will be needed. When the refresh SSL operation is performed, any running SSL channels are stopped and restarted. This can take a while but the MQ Explorer will only wait for 30 seconds at which point you will see error message AMQ4562. The refresh will continue and the channels will be restarted so you should see them go to a running state after a while.

5. Display the channel status on QM8 using **runmqsc QM8** then enter command:

```
DIS CHS(QM8.TO.QMC*) SSLCERTI SSLPEER
```

You should see QM8.TO.QMC.CHL2 is using 'ALL QMGR cert2', whereas QM8.TO.QMC is using 'QM8 CHL cert'.

QM8.TO.QMC uses the certificate specified in the CERTLABEL field of the channel definition. For QM8.TO.QMC.CHL2 we left the channel definition for CERTLABEL blank so it is using the certificate specified in the queue manager property CERTLABEL.

```
Command Prompt - runmqsc QM8
C:\Users\ibmdemo.DESKTOP-6DSOOH2\runmqsc QM8
5724-H72 (C) Copyright IBM Corp. 1994, 2018.
Starting MQSC for queue manager QM8.

DIS CHS(QM8.TO.QMC.CHL2) SSLCERTI SSLPEER
  1 : DIS CHS(QM8.TO.QMC.CHL2) SSLCERTI SSLPEER
AMQ8417I: Display Channel Status details.
  CHANNEL(QM8.TO.QMC.CHL2)          CHLTYPE(SDR)
  CONNAME(127.0.0.1(1444))          CURRENT
  RQMNAME(QMC)
  SSLCERTI(CN=ALL QMGR cert2,OU=MQPOT,O=IBM)
  SSLPEER(SERIALNUMBER=54:DC:A8:3E,CN=ALL QMGR cert2,OU=MQPOT,O=IBM)
  STATUS(RUNNING)                  SUBSTATE(MQGET)
  XMITQ(QMC.XMITQ.CHL2)


```

This concludes Lab 7.

Return MQ Basic Menu ([mq_basic_pot_overview.html](#))

©2019 IBM. All rights reserved.

Site last generated: Apr 19, 2019

