Using SSL to connect MQ Explorer and MQ Java clients to a queue manager in WebSphere MQ 7.1/7.5

IBM Techdoc: 7041559

http://www.ibm.com/support/docview.wss?rs=171&uid=swg27041559

Date last updated: 17-Mar-2014

Angel Rivera – rivera@us.ibm.com
IBM WebSphere MQ Support

+++ Objective

The objective of this document is to provide the step-by-step details for connecting the WebSphere MQ Explorer and MQ Java clients 7.1/7.5 from one workstation (such as running in Windows) to a queue managers running on another workstation, using SSL.

To provide better background, because the MQ Explorer uses the MQ classes for Java, it is necessary to cover also the setup for an MQ client that uses the MQ classes for Java.

The chapters are:
Chapter 1: Connecting MQ Java client to a single-instance queue manager with SSL
Chapter 2: Connecting MQ Explorer to a single-instance queue manager with SSL

See the following companion techdoc:

http://www.ibm.com/support/docview.wss?rs=171&uid=swg27041551
Using SSL to connect MQ C-based client to a queue manager in WebSphere MQ 7.1 and 7.5

This document uses the SSL commands that are provided in MQ 7.1 and 7.5. The SSL commands in MQ 7.0 were renamed in MQ 7.1 and 7.5.

The following techdoc shows the SSL commands used in MQ 7.0:
http://www.ibm.com/support/docview.wss?rs=171&uid=swg27038221
Using SSL to connect MQ Explorer to Single-instance and Multi-Instance queue managers in WebSphere MQ 7.0

++ Regarding certificate label

The certificate label is the concatenation of the following (in lowercase):

Client:	ibmwebspheremq + clientName
Queue Manager:	ibmwebspheremq + queueManagerName

+++ Configuration

a) MQ Explorer 7.5.0.2 running in Windows 7

b) Single-instance queue manager running 7.5.0.3 in Linux Intel 32-bit (with SSL)
Name: MFT_LNX Hostname: veracruz.x.com Port: 1424
SSL enabled server-connection channel: SSL.SVRCONN

c) The following SSL Cipher will be used:
NULL_SHA (SSL_RSA_WITH_NULL_SHA)

+++ Summary of steps for the SSL configuration

Step 1: Client: Create SSL client key database
Step 2: Client: Create certificate
Step 3: Client: Extract the public SSL client certificate and copy it to the SSL server side
Step 4: Server: Create SSL server key database
Step 5: Server: Create certificate
Step 6: Server: Add the SSL client certificate to the Queue Manager's key database.
Step 7: Server: Extract the public SSL server certificate and copy it to the SSL client side
Step 8: Client: Add the SSL client certificate to the Client's key database.
Step 9: Server: Run MQSC commands for SSL server side queue manager
Step 10: Client: Run sample client to test connection

+++ Testing Samples

Download the following SupportPac.
In this document, the SupportPac was downloaded in:
C:\MQ-SupportPac\MO04 SSL Wizard

Notice that we are going to use the testing samples only, which work for 7.1 and 7.5. The GUI that is provided for the SSL Wizard function has not been updated to use the GSKit commands used by MQ 7.1 and 7.5.

http://www-1.ibm.com/support/docview.wss?uid=swg24010367
MO04: WebSphere MQ SSL Wizard

++
+++ Chapter 1: Connecting MQ Java client to a single-instance queue manager
+++ with SSL
++

In this chapter, we will explore the scenario in which SSL is used to connect an MQ Java client application to a remote queue manager.

The scenario for using the MQ Explorer is covered in Chapter 2.

The idea is to start with the simplest scenario, without adding additional players. If there is a problem, the troubleshooting will be done on the minimum amount of players.

+++ Step 1: Client: Create SSL client key database

WINDOWS:
Log in as an MQ Administrator:

Note that in the Windows host used for this testing, the version is Windows 7 and there are multiple versions of MQ installed.
The corresponding directory for MQ 7.5 in this machine is:
cd C:\Program Files (x86)\IBM\WebSphere MQ_2

Open a command Prompt.

Because this Windows machine has several versions of MQ, it is necessary to establish the environment for MQ 7.5:

"C:\Program Files (x86)\IBM\WebSphere MQ_2\bin\setmqenv" -n Installation2

Change to the directory where the Client key database will be located:
cd C:\Program Files\IBM\WebSphere MQ\

WINDOWS:
Create SSL client key database type jks (to be used with Java and JMS programs)

runmqckm -keydb -create -db "C:\Program Files (x86)\IBM\WebSphere MQ_2\rivera.jks" -pw clientpass -type jks

Note that the actual key database is created in a different directory in Windows 7:
%USERPROFILE%\AppData\Local\VirtualStore\

In this case:

cd "C:\Users\IBM_ADMIN\AppData\Local\VirtualStore\Program Files (x86)\IBM\WebSphere MQ_2"

dir
03/07/2014 01:00 PM 32 rivera.jks (new file)

+++ Step 2: Client: Create certificate

WINDOWS:
SSL client certificate setup

Create the certificate:

runmqckm -cert -create -db "C:\Users\IBM_ADMIN\AppData\Local\VirtualStore\Program Files (x86)\IBM\WebSphere MQ_2\rivera.jks" -pw clientpass -label ibmwebspheremqrivera -dn "CN=rivera,OU=Support,O=IBM,ST=NC,C=" -expire 365

Notice that the file size for the jks file increased:

dir
03/07/2014 01:08 PM 1,309 rivera.jks (increase in file size)

List the certificate:

Ouptut:
Certificates in database C:\Users\IBM_ADMIN\AppData\Local\VirtualStore\Program F iles (x86)\IBM\WebSphere MQ_2\rivera.jks:
  ibmwebspheremqrivera

+++ Step 3: Client: Extract the public SSL client certificate and copy it to the SSL server side

WINDOWS:
Extract the public SSL client certificate
A new file is created in the current directory: rivera.crt

runmqckm -cert -extract -db "C:\Users\IBM_ADMIN\AppData\Local\VirtualStore\Program Files (x86)\IBM\WebSphere MQ_2\rivera.jks" -pw clientpass -label ibmwebspheremqrivera -target rivera.crt -format ascii

dir
03/09/2014 07:37 AM 776 rivera.crt (new file)
03/07/2014 02:08 PM 1,309 rivera.jks
WINDOWS:
Copy the public SSL client certificate to the SSL server side
FTP the file rivera.crt in ASCII mode from Windows to Linux into the directory:
/var/mqm/qmgrs/MFT_LNX/ssl

ftp veracruz.x.com
User xxx
Password: xxx
ftp> **ascii**
ftp> **cd /var/mqm/qmgrs/MFT_LNX/ssl**
ftp> **put rivera.crt**
ftp> **quit**

+++ Step 4: Server: Create SSL server key database

UNIX:
Create SSL server key database

runmqckm -keydb -create -db "/var/mqm/qmgrs/MFT_LNX/ssl/MFT_LNX.kdb" -pw serverpass -type cms -expire 365 -stash

These are the files that are created:
ls -l /var/mqm/qmgrs/MFT_LNX/ssl
-rw------- 1 rivera mqm 80 2014-03-07 13:11 MFT_LNX.kdb
-rw------- 1 rivera mqm 80 2014-03-07 13:11 MFT_LNX.rdb
-rw------- 1 rivera mqm 129 2014-03-07 13:11 MFT_LNX.sth

+++ Step 5: Server: Create certificate

UNIX:
Create certificate:

runmqckm -cert -create -db "/var/mqm/qmgrs/MFT_LNX/ssl/MFT_LNX.kdb" -pw serverpass -label ibmwebspheremqmft_lnx -dn "CN=MFT_LNX,OU=Support,O=IBM,ST=NC,C=" -expire 365

List the certificate:

runmqckm -cert -list -db "/var/mqm/qmgrs/MFT_LNX/ssl/MFT_LNX.kdb" -pw serverpass

Output:
Certificates in database /var/mqm/qmgrs/MFT_LNX/ssl/MFT_LNX.kdb:
  ibmwebspheremqmft_lnx

Notice that the file size for the kdb file was increased
ls -l
-rw------- 1 rivera mqm 5080 2014-03-07 13:18 MFT_LNX.kdb (increased file size)
-rw------- 1 rivera mqm 80 2014-03-07 13:18 MFT_LNX.rdb
-rw------- 1 rivera mqm 129 2014-03-07 13:11 MFT_LNX.sth

+++ Step 6: Server: Add the SSL client certificate to the Queue Manager's key database.

UNIX:
Add the client certificate
Change to the directory where the key database is located:

cd /var/mqm/qmgrs/MFT_LNX/ssl/

Notice that the file rivera.crt is in the directory:
ls -l
-rw------- 1 rivera mqm 5080 2014-03-07 13:18 MFT_LNX.kdb
-rw------- 1 rivera mqm 80 2014-03-07 13:18 MFT_LNX.rdb
-rw------- 1 rivera mqm 129 2014-03-07 13:11 MFT_LNX.sth
-rw------- 1 rivera mqm 776 2014-03-09 07:49 rivera.crt

Add the certificate rivera.kdb:

runmqckm -cert -add -db "/var/mqm/qmgrs/MFT_LNX/ssl/MFT_LNX.kdb" -pw serverpass -label ibmwebspheremqrivera -file rivera.crt -format ascii

List the certificates:

runmqckm -cert -list -db "/var/mqm/qmgrs/MFT_LNX/ssl/MFT_LNX.kdb" -pw serverpass
Output:
Certificates in database /var/mqm/qmgrs/MFT_LNX/ssl/MFT_LNX.kdb:
  ibmwebspheremqmft_lnx
  ibmwebspheremqrivera

Notice the increase in size for the kdb file:
ls -l
-rw------- 1 rivera mqm 10080 2014-03-09 07:53 MFT_LNX.kdb (increase in file size)
-rw------- 1 rivera mqm 80 2014-03-09 07:53 MFT_LNX.rdb
-rw------- 1 rivera mqm 129 2014-03-07 13:11 MFT_LNX.sth
-rw------- 1 rivera mqm 776 2014-03-09 07:49 rivera.crt

+++ Step 7: Server: Extract the public SSL server certificate and copy it to the SSL client side

UNIX:
Extract the public SSL server certificate and copy it to the SSL client side

cd /var/mqm/qmgrs/MFT_LNX/ssl/

runmqckm -cert -extract -db "/var/mqm/qmgrs/MFT_LNX/ssl/MFT_LNX.kdb" -pw serverpass -label ibmwebspheremqmft_lnx -target MFT_LNX.crt -format ascii

The file "MFT_LNX.crt" is created in the current directory

ls -l

```
-rw------- 1 rivera mqm   840 2014-03-09 07:55 MFT_LNX.crt (new file)
-rw------- 1 rivera mqm 10080 2014-03-09 07:53 MFT_LNX.kdb
-rw------- 1 rivera mqm    80 2014-03-09 07:53 MFT_LNX.rdb
-rw------- 1 rivera mqm   129 2014-03-07 13:11 MFT_LNX.sth
-rw------- 1 rivera mqm   776 2014-03-09 07:49 rivera.crt
```

+++ Step 8: Client: Add the SSL client certificate to the Client's key database.

WINDOWS:
Copy the public SSL server certificate to the SSL client side
FTP MFT_LNX.crt in ASCII mode from veracruz.x.com from directory:
  /var/mqm/qmgrs/MFT_LNX/ssl/
to directory:
  C:\Users\IBM_ADMIN\AppData\Local\VirtualStore\Program Files (x86)\IBM\WebSphere MQ_2

cd "C:\Users\IBM_ADMIN\AppData\Local\VirtualStore\Program Files (x86)\IBM\WebSphereMQ_2"

ftp veracruz
ftp> **ascii**
ftp> **cd /var/mqm/qmgrs/MFT_LNX/ssl**
ftp> **get MFT_LNX.crt**
ftp> **quit**

Notice the new file:

dir
03/09/2014 07:51 AM 840 MFT_LNX.crt (new file)
03/09/2014 07:37 AM 776 rivera.crt
03/07/2014 02:08 PM 1,309 rivera.jks

WINDOWS:
Add the SSL client certificate to the Queue Manager's key database.

runmqckm -cert -add -db "C:\Users\IBM_ADMIN\AppData\Local\VirtualStore\Program Files (x86)\IBM\WebSphere MQ_2\rivera.jks" -pw clientpass -label ibmwebspheremqmft_lnx -file MFT_LNX.crt -format ascii

List the certificate:
runmqckm -cert -list -db "C:\Users\IBM_ADMIN\AppData\Local\VirtualStore\Program Files (x86)\IBM\WebSphere MQ_2\rivera.jks" -pw clientpass
Output:
Certificates in database C:\Users\IBM_ADMIN\AppData\Local\VirtualStore\Program F iles (x86)\IBM\WebSphere MQ_2\rivera.jks:
  ibmwebspheremqmft_lnx
  ibmwebspheremqrivera

Notice the increase in the size of the jks file:

dir

```
03/09/2014  07:51 AM            840 MFT_LNX.crt
03/09/2014  07:37 AM            776 rivera.crt
03/09/2014  07:54 AM          1,926 rivera.jks (increase in file size)
```

+++ Step 9: Server: Run MQSC commands for SSL server side queue manager

UNIX:
Run MQSC commands for SSL server side queue manager MFT_LNX
runmqsc MFT_LNX

You MUST provide the value for SSLKEYR as follows: full path name of the key store MINUS the .kdb suffix (the .kdb is added at runtime):
Full path name with suffix: /var/mqm/qmgrs/MFT_LNX/ssl/MFT_LNX.kdb
Full path name minus suffix: /var/mqm/qmgrs/MFT_LNX/ssl/MFT_LNX

```
ALTER QMGR SSLKEYR('/var/mqm/qmgrs/MFT_LNX/ssl/MFT_LNX')
ALTER QMGR SSLFIPS(NO)
DEFINE CHANNEL('SSL.SVRCONN') CHLTYPE(SVRCONN) TRPTYPE(TCP) +
SSLCIPH(NULL_SHA) SSLCAUTH(REQUIRED) REPLACE
REFRESH SECURITY TYPE(SSL)
end
```

UNIX:
Ensure that the key database has the proper file permissions for the user mqm
In this test, the userid 'rivera' (who belongs to the 'mqm' groupid and thus, is an MQ Administrator) is the one that issued the GSKit commands.
But the files that were created will not allow the userid 'mqm' to work with them, causing runtime problems.

```
cd /var/mqm/qmgrs/MFT_LNX/ssl
ls -l
-rw------- 1 rivera mqm   840 2014-03-09 07:55 MFT_LNX.crt
-rw------- 1 rivera mqm 10080 2014-03-09 07:53 MFT_LNX.kdb
-rw------- 1 rivera mqm    80 2014-03-09 07:53 MFT_LNX.rdb
-rw------- 1 rivera mqm   129 2014-03-07 13:11 MFT_LNX.sth
-rw------- 1 rivera mqm   776 2014-03-09 07:49 rivera.crt
```

Thus, it is necessary to alter the file permissions for the users in the group to be able to read-write:

```
chmod 660 *
ls -l
-rw-rw---- 1 rivera mqm   840 2014-03-09 07:55 MFT_LNX.crt
-rw-rw---- 1 rivera mqm 10080 2014-03-09 07:53 MFT_LNX.kdb
-rw-rw---- 1 rivera mqm    80 2014-03-09 07:53 MFT_LNX.rdb
-rw-rw---- 1 rivera mqm   129 2014-03-07 13:11 MFT_LNX.sth
-rw-rw---- 1 rivera mqm   776 2014-03-09 07:49 rivera.crt
```

+++ Step 10: Client: Run sample client to test connection

WINDOWS:
Run the Java sample client

Use the command prompt that points to:
cd C:\MQ-SupportPac\MO04 SSL Wizard

cd client_samples\bin

SSLSample (Java)

java SSLSample veracruz.x.com 1424 SSL.SVRCONN MFT_LNX SSL_RSA_WITH_NULL_SHA "C:\Users\IBM_ADMIN\AppData\Local\VirtualStore\Program Files (x86)\IBM\WebSphere MQ_2\rivera.jks" clientpass

```
Connecting to:
  Conname = veracruz.x.com
  Port = 1424
  Channel = SSL.SVRCONN
  Qmgr = MFT_LNX
  SSLCiph = SSL_RSA_WITH_NULL_SHA
  SSLTrustStore = C:\Users\IBM_ADMIN\AppData\Local\VirtualStore\Program Files (x
86)\IBM\WebSphere MQ_2\rivera.jks
  SSLKeyStore = C:\Users\IBM_ADMIN\AppData\Local\VirtualStore\Program Files (x86
)\IBM\WebSphere MQ_2\rivera.jks
  SSLKeyStorePassword = clientpass
Connecting...
Connection successful!
Disconnecting from the Queue Manager
Done!
```

++
+++ Chapter 2: Connecting MQ Explorer to a single-instance queue manager with SSL
++

The MQ Explorer connects to remote queue managers using an MQI channel.

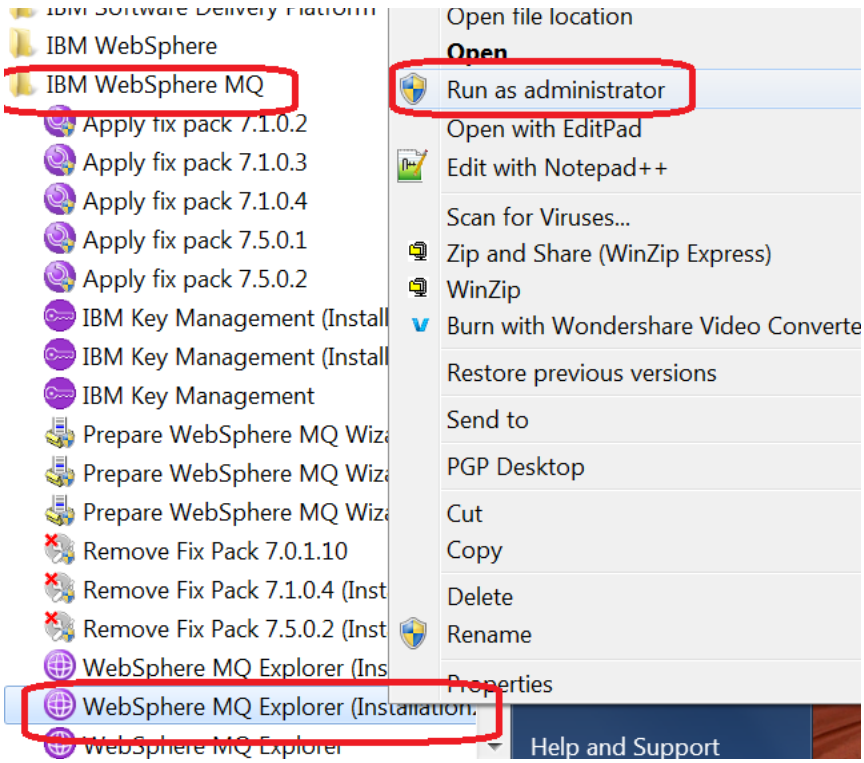
Notes:
- See Chapter 1 for the steps to create the key database and the certificates.
- Only the additional steps that are applicable for the MQ Explorer will be included here.

WINDOWS:
Tasks on the system that hosts the WebSphere MQ Explorer

On the system hosting the WebSphere MQ Explorer, perform the following tasks:

On Windows and Linux systems, start MQ Explorer by using the system menu, the MQExplorer executable file, or the strmqcfg command.

WARNING: In Windows 7 you must start the MQ Explorer as an Administrator!
Start > Programs >IBM WebSphere MQ > WebSphere MQ Explorer
Right click and selct “Run as administrator”



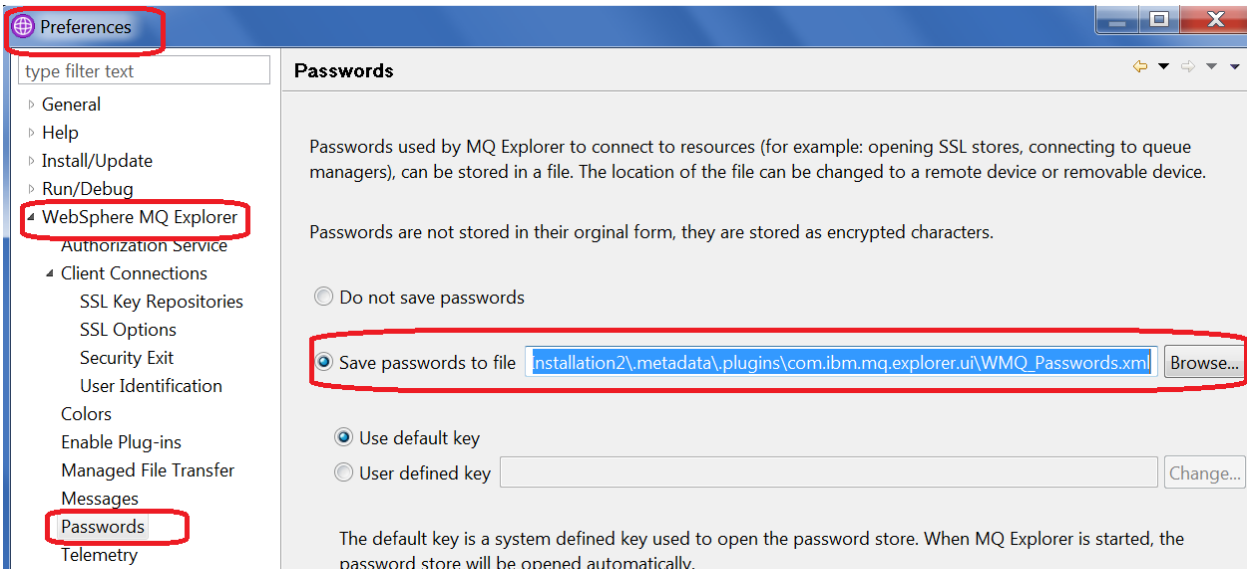
From the WebSphere MQ Explorer toolbar, click Window -> Preferences, then expand WebSphere MQ Explorer.

Let's enable Passwords:
Select Passwords on the left panel, then
enabled

The reason for this step is that if you do not save the passwords in this Preference page, then every time that the MQ Explorer tries to connect or reconnect to the multi-instance queue manager, the MQ Explorer will prompt you for the password of the key store.

Select: Window > Preferences > WebSphere MQ Explorer > Passwords
The default is: (*) Do not save passwords

Enable:
(*) Save passwords to file



The default file to save the passwords is:

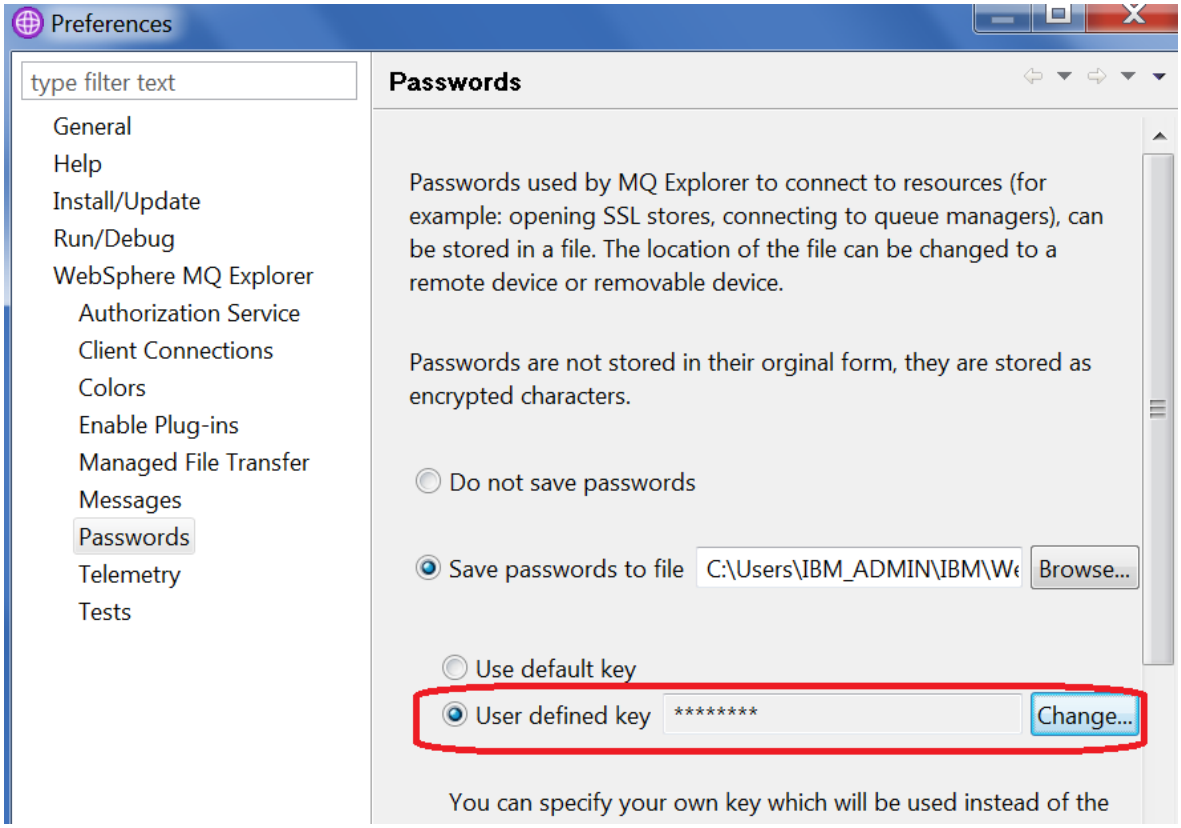
C:\Users\IBM_ADMIN\IBM\WebSphereMQ\workspace-Installation2\.metadata\.plugins\com.ibm.mq.explorer.ui\WMQ_Passwords.xml

Then there is a further default which is:
(*) Use default key
( ) User defined key

It was changed to:
() Use default key
(*) User defined key

I entered the value that I used in the techdoc:
clientpass

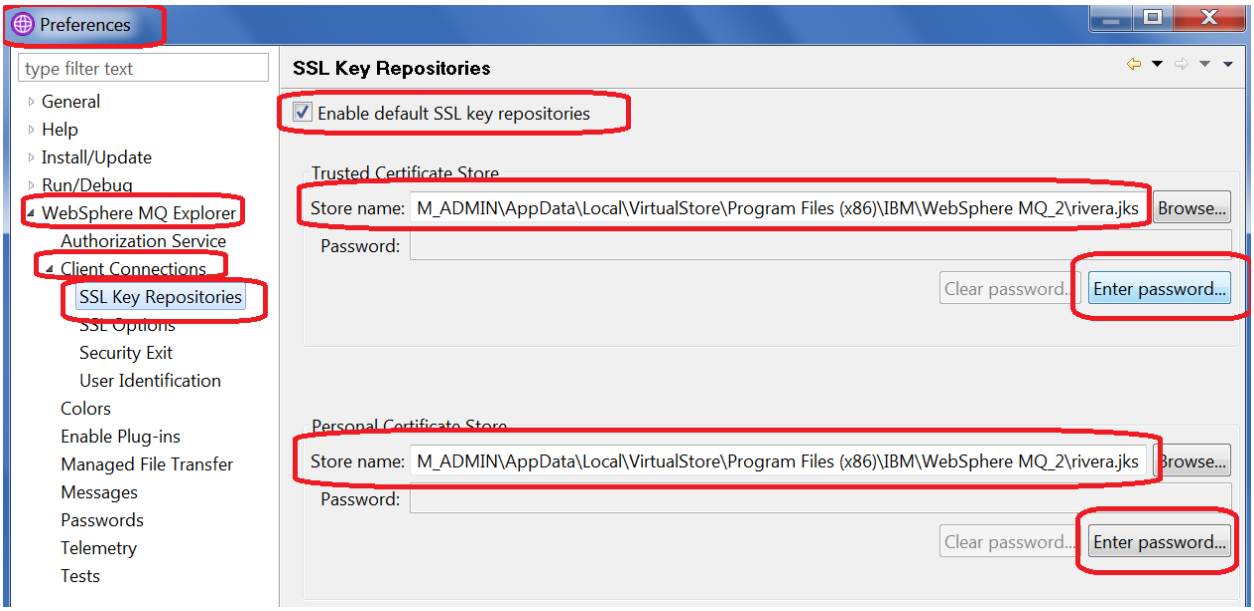
Click Apply



Now specify the SSL Key Repositories
Select Client Connections from the left panel, then
click SSL Key Repositories.

Click on the checkbox:
(*) Enable default SSL key repositories

For the 2 fields highlighted below:
  Trusted Certificate Store
  Personal Certificate Store
… enter the following for the JKS file created previously, then click OK:
Name:
C:\Users\IBM_ADMIN\AppData\Local\VirtualStore\Program Files (x86)\IBM\WebSphere MQ_2\rivera.jks
Password: clientpass

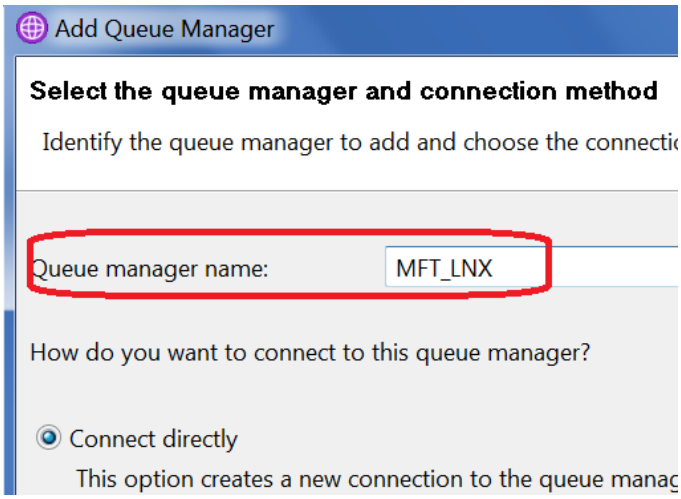


Close the Preferences window

A side effect of saving the passwords is that every time that you start the MQ Explorer, you will be asked to enter the password of the key store, but after that, during the duration of the MQ Explorer session, you will not be asked for the password.

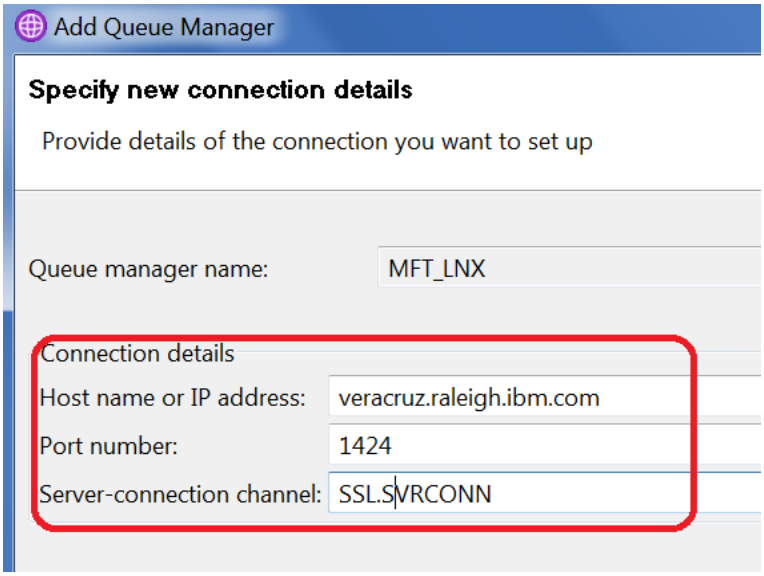
In the left panel, select Queue Managers.
Right-click and select “Add Remote Queue Manager...”.

Specify the "Queue manager name": MFT_LNX
And accept the default way to connect to it:
(*) Connect directly



Click Next.

Specify the host name: veracruz.x.ibm.com
Port number: 1424
Server-connection channel: SSL.SVRCONN
This channel was created in Chapter 1.

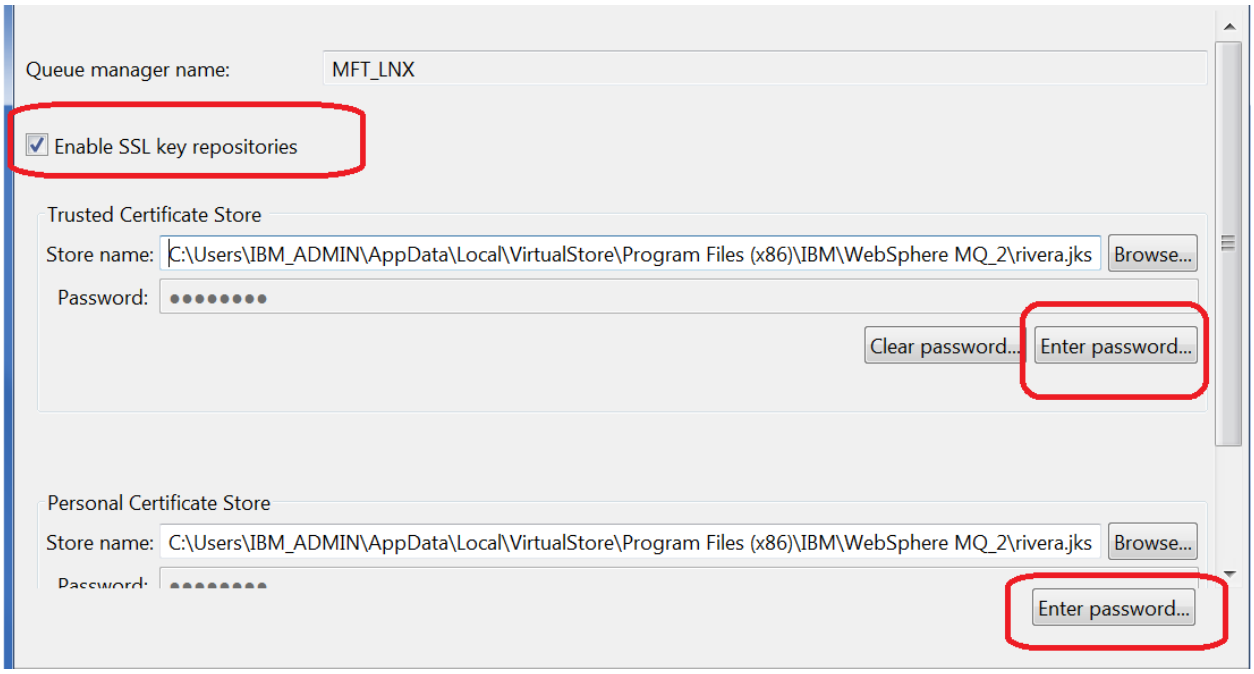


Click Next.
For the next screen "Specify security exit details", click Next.

For the next screen "Specify user identification details", click Next.

For the next screen "Specify SSL certificate key repository details ", because you pre-filled the Preferences page with the SSL certificate stores, the screen will show the *.jks files that were defined.

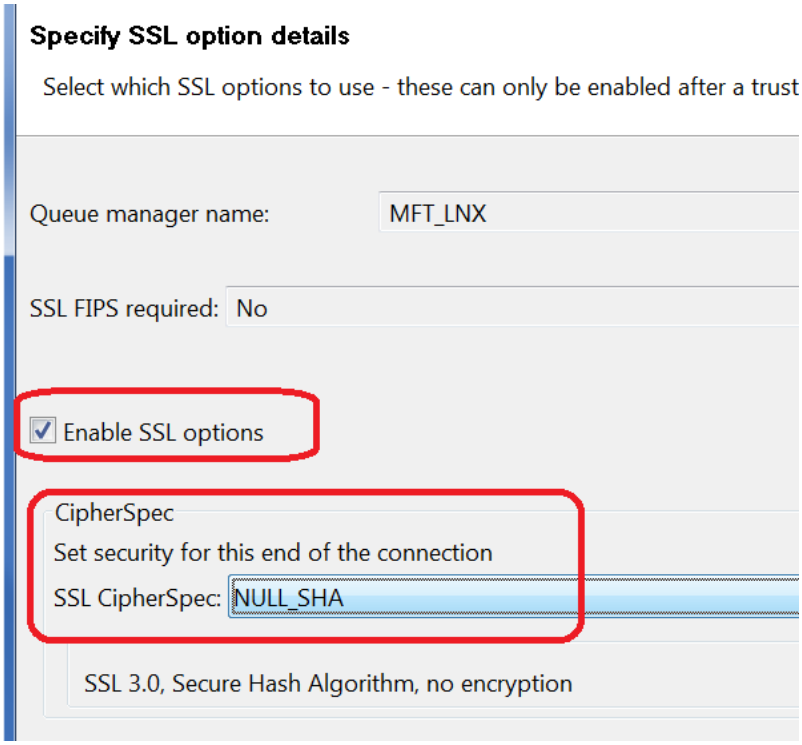
Ensure that the checkbox for the following is selected:
(*) Enable SSL key repositories
And specify the key stores:
C:\Users\IBM_ADMIN\AppData\Local\VirtualStore\Program Files (x86)\IBM\WebSphere MQ_2\rivera.jks
Password: clientpass



Click Next.

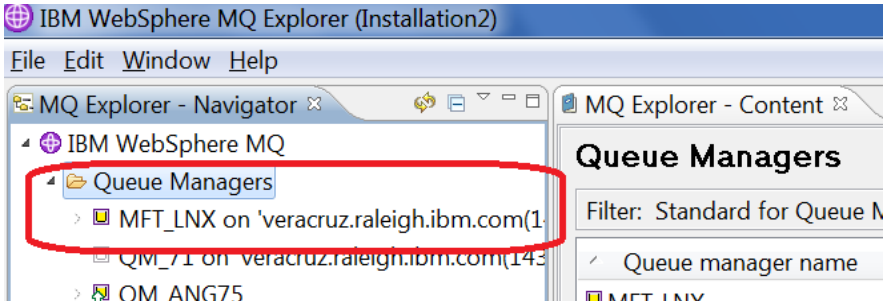
For the screen "Specify SSL option details":

Select the checkbox for:
(*) Enable SSL options
Select the CipherSpec for:
NULL_SHA



Click Finish.

Notice the new entry in the Navigator for the queue manager:
MFT_LNX on 'veracruz.raleigh.ibm.com(1424)'



You have completed the steps for successfully using the MQ Explorer to connect to a remote queue manager using SSL. Yeah!

+++ end +++