# How to connect IBM MQ Explorer to Remote IBM Cloud Queue Manager

<https://cloud.ibm.com/docs/mqcloud?topic=mqcloud-mqoc_configure_chl_ssl#keystore_jks_mac>

## Prerequisites

* You have MQ Explorer installed on your remote machine.
* You have a MQ IBM Cloud Queue Manager deployed

## Download the Queue Manager Certificate.

You must download the cert from the keystore on the IBM Cloud Queue Manager. The download will be in the format of a PEM file. You need to use the cert that is associated with the queue manager.

**Note**: *The default cert that is associated with the queue manager is labeled qmgrcert*

A computer screen with a red arrow pointing to a blue box

Description automatically generated

## Create a java keystore

Below is an example of the keytool command to convert the CERT (your downloaded pem file) into a jks keystore.

keytool -importcert -file qmgrcert.pem -alias qmgrcert -keystore key.jks -storepass <your password>

To view the keystore you can run this command below

Keytool -list -keystore key.jks -storepass <your password>

## Reset the IBM Cloud API Key if you do not have the key already.

You can find a button in the bottom right hand corner when you look at the following admin screen on IBM Cloud.

**Note**: *Download the apikey, you will only get one chance to view it.*

A screenshot of a computer

Description automatically generated

## Configure a remote queue manager in MQ Explorer

Open up MQ Explorer on your remote workstation. Right click and add a new remote queue manager.

You will need to supply the correct connection information as showed in the below example.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

The screen shot below is where you need to enter the apikey for your admin user. This should be in the file you downloaded when you rest the API Key.

A screenshot of a computer

Description automatically generated

You need to enable TLS security and point both the personal keystore and the trusted keystore to your repository, which is the jks file.

The keystore has a password. You actually set that password in the first step. You will need to enter the password for your keystore for both the private and trusted stores.

A screenshot of a computer

Description automatically generated

The ciper spec should match what you have on the MQ Server.

**Note**: *The default is ANY\_TLS12\_OR\_HIGHER*

A screenshot of a computer

Description automatically generated

You should now be able to connect.