Configuring a Secure Connection for the IBM MQ Web Console on Linux and Windows Platforms

https://www.ibm.com/support/pages/node/6985659

Date last updated: 24-Apr-2023

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

PURPOSE

The purpose of this document is to provide instructions to configure the MQ Console implementing a secure connection (https).

REQUIREMENTS

These instructions assume the reader has a basic knowledge and skills with the MQ product, browsers, and IBM's Global Secuirty Kit (GSKit) certificate management tool.

SUMMARY

1. Install the MQ Console
2. Replace the existing configuration file, mqwebuser.xml with the basic registry sample file that is configured to offer basic security.
3. Start the mqweb server that supports MQ Console.
4. Confirm the MQ Console web server has started on port 9443.
5. When you start the mqweb server a self-signed personal certificate in a key repository will be generated at the following locations.
6. Extract the signer certificate from the self-signed personal certificate, to a file using the following commands.
7. Add the signer certificate default.cer to your browser of choice (Chrome Browser Example).
8. From step 4 use the https address to access MQ Console from your browser.
9. Login to the MQ Console using the default administrator's userId/password.
10. Configure the MQ Web Server to accept remote connections.
11. Browser Requirements to allow the MQ Console to connect remote to the MQ Web Server.
12. Creating a new self-signed certificate using a full hostname or IP Address.
13. Extracting the root signer certificate from the newly generated self-signed certificate.
14. Restart your MQ Web Server so that the new certificate is used in the connection.
15. Make sure the values set in your CN or SAN certificate distinguished name properties (full hostname or ip address) is used to configure your MQ Web Console https connection.

PROCEDURE

Configuring a basic one-way secure connection to the IBM MQ Web Console using self-signed certificates.

NOTE: One way authentication is when the initiating side of the connection authenticates the receiving side of the connection. In this case, the MQ Web Console (Browser) authenticates the MQ Web Server.

1. Install the MQ Console:

a. On Linux: Install the MQSeriesWeb component. For more information about installing components on Linux, see Linux installation tasks.

b. On Windows: Install the Web Administration feature. For more information about installing features on Windows, see Windows installation tasks.

2. Replace the existing configuration file, mqwebuser.xml with the basic registry sample file that is configured to offer basic security.

a. On Linux: Copy the basic_registry.xml file from the /MQ_INSTALLATION_PATH/web/mq/samp/configuration directory to the directory /var/mqm/web/installations/installationName/servers/mqweb
Rename the original mqwebuser.xml file and then rename the basic_registry.xml file to mqwebuser.xml.

b. On Windows: Copy the basic_registry.xml file from \MQ_INSTALLATION_DIRECTORY\web\mq\samp\configuration directory to the directory \MQ_DATA_PATH\web\installations\InstallationName\servers\mqweb
Rename the original mqwebuser.xml file and then rename the basic_registry.xml file to mqwebuser.xml.

NOTE: The basic_registry.xml sample file configures four user rolls:

mqadmin - An administrative user that is a member of the MQWebAdmin role.
mqreader - A read-only administrative user that is a member of the MQWebAdminRO role.
mftadmin - An administrative user that is a member of the MFTWebAdmin role.
mftreader - A read-only administrative user that is a member of the MFTWebAdminRO role.

3. Start the mqweb server that supports MQ Console:

On Linux and Windows, as a privileged user, enter the following command: strmqweb

Example of the mqweb server that has started:

```
C:\>strmqweb
Starting server mqweb.
Server mqweb started.
```

NOTE: A privileged user on Linux would be root, mqm, or a userId in the mqm group.
A privileged user on Windows would be Administrator and any userId or domain_mqm group in the mqm local group.

4. Confirm the MQ Console web server has started on port 9443 by entering the following command: dspmqweb.

```
C:\>dspmqweb
MQWB1124I: Server 'mqweb' is running.
URLS:
  https://localhost:9443/ibmmq/rest/
  https://localhost:9443/ibmmq/console/
```

5. When you start the mqweb server a self-signed personal certificate in a key repository will be generated at the following locations:

a. On Linux:
/var/mqm/web/installations/InstallationName/servers/mqweb/resources/security/key.jks

b. On Windows:
\MQ_DATA_PATH\web\installations\InstallationName\servers\mqweb\resources\security\key.jks directory

6. Extract the signer certificate from the self-signed personal certificate, to a file using the following commands:

On Linux and Windows:

runmqckm -cert -extract -db "The Path referenced above to key.jks" -pw password -label default -target public.cer

or

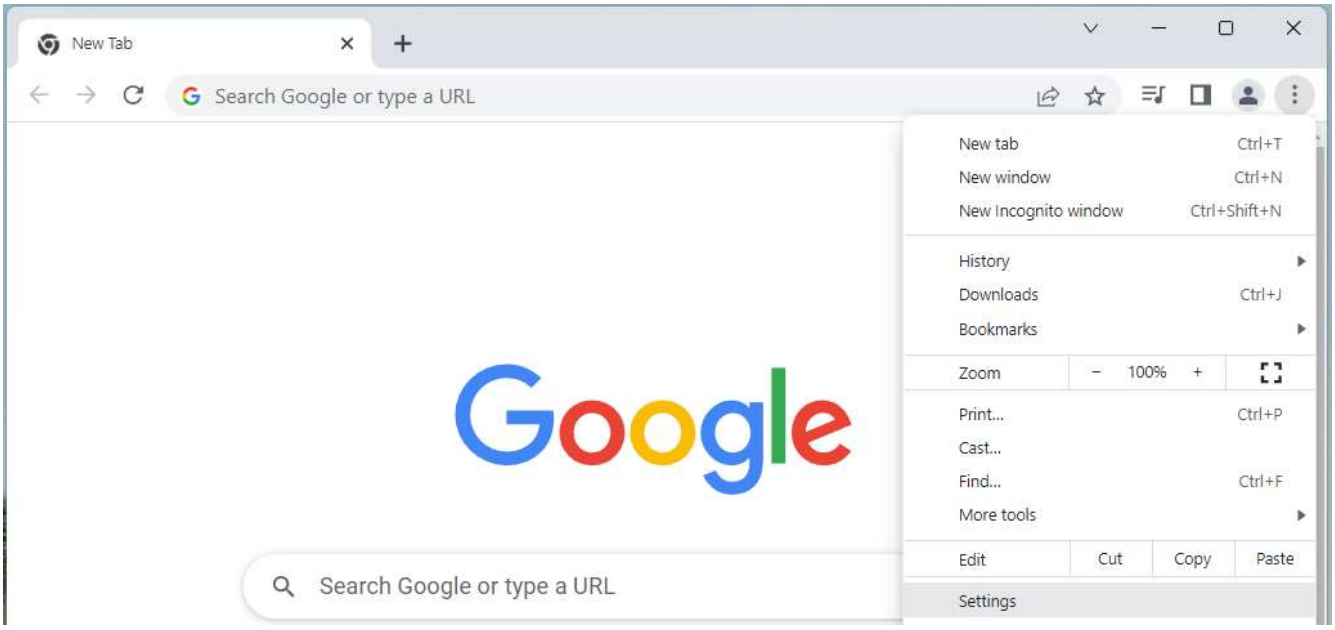
keytool -export -alias default -keystore "Fully Qualified Path referenced above" -rfc -file default.cer

Enter key.jks repository password

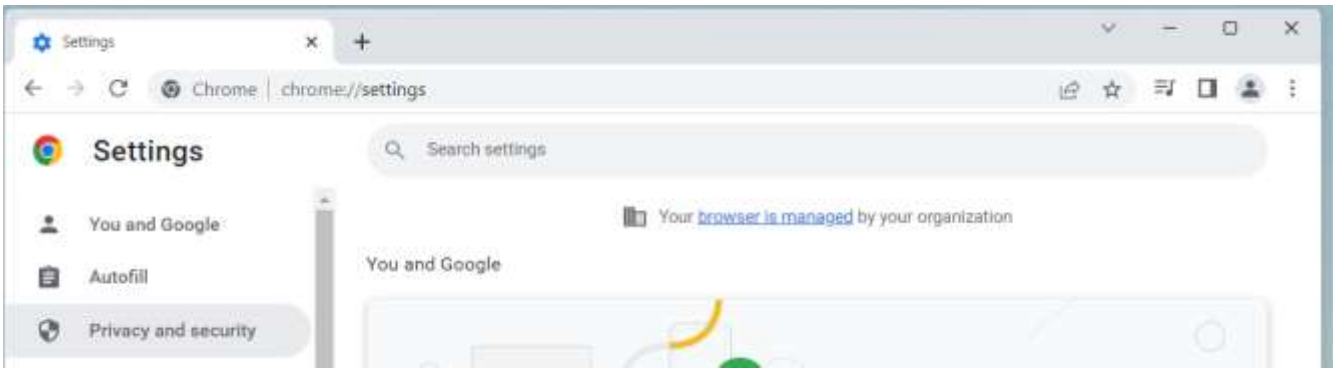
NOTE:
The default password for the key.jks repository is password.
The self-signed personal certificate is named default.

7. Add the signer certificate default.cer to your browser of choice. Below are the steps for a Chrome browser as an example:

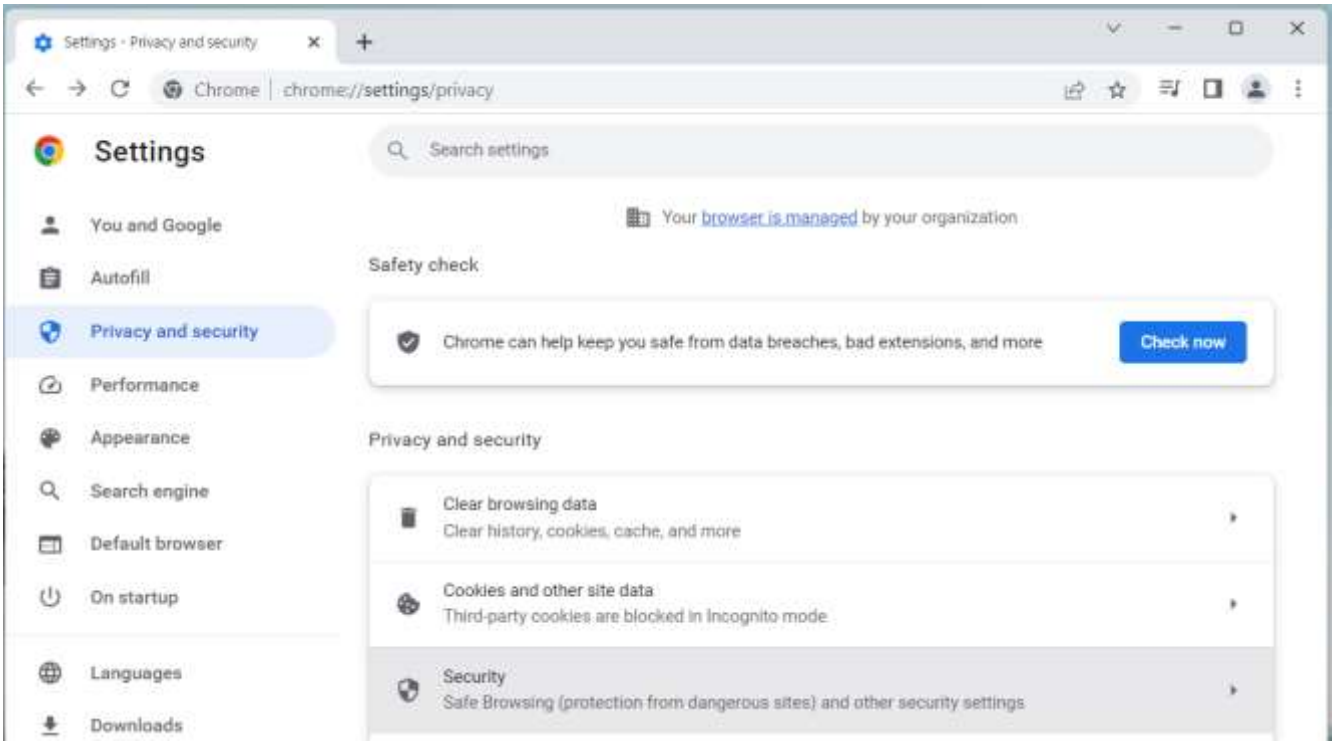
a) Select settings from the veritical 3 dots icon drop down menu.



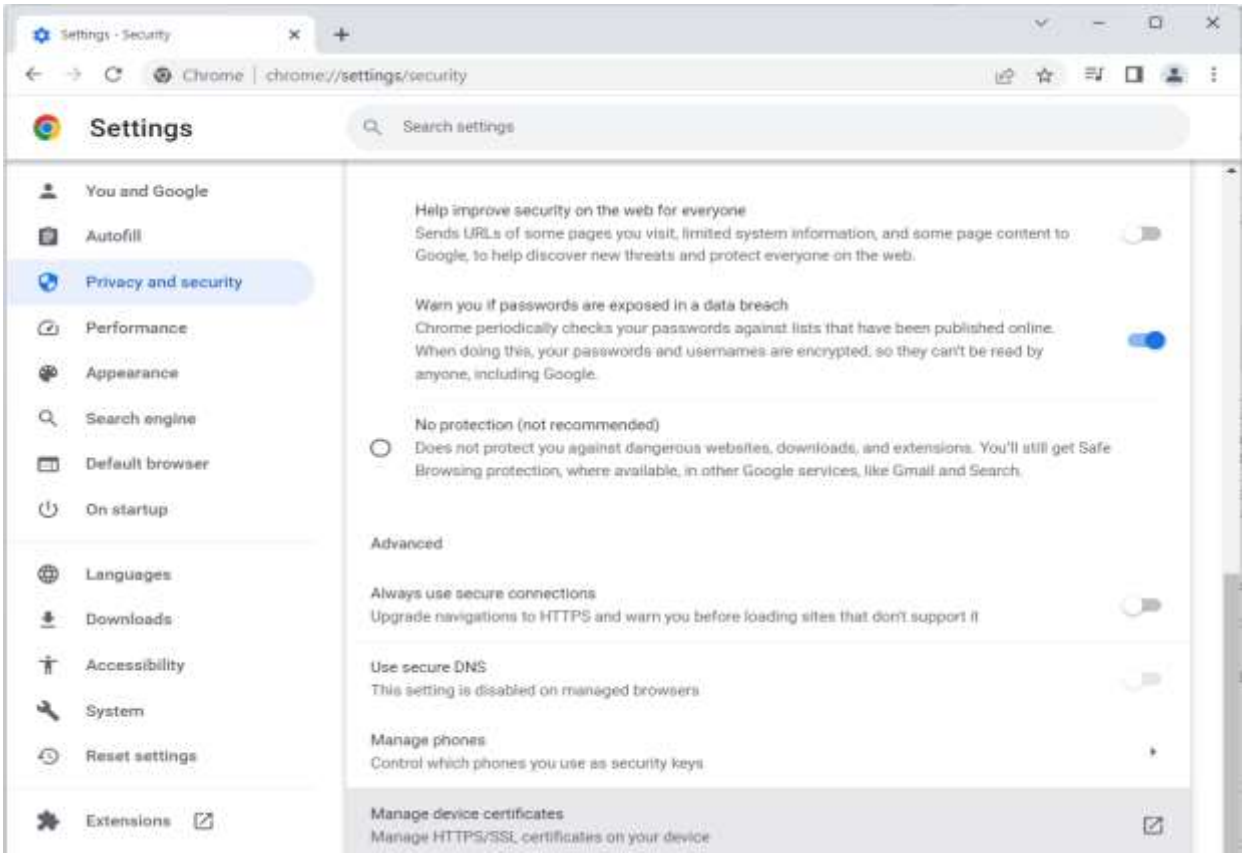
b) From the Settings select "Privacy and security ".



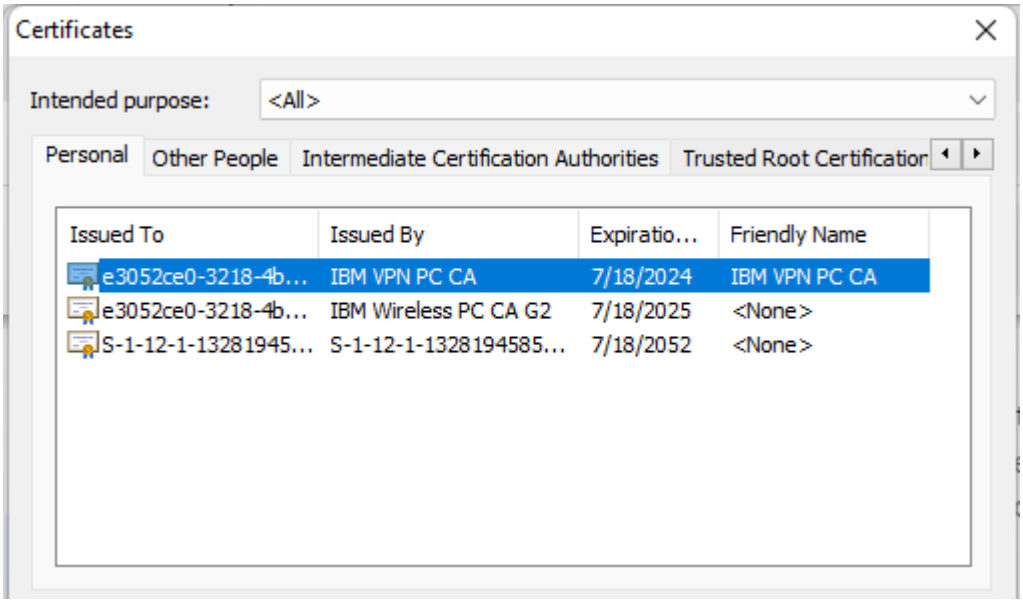
c) Scroll down and click "Security". click on "Manage certificates".



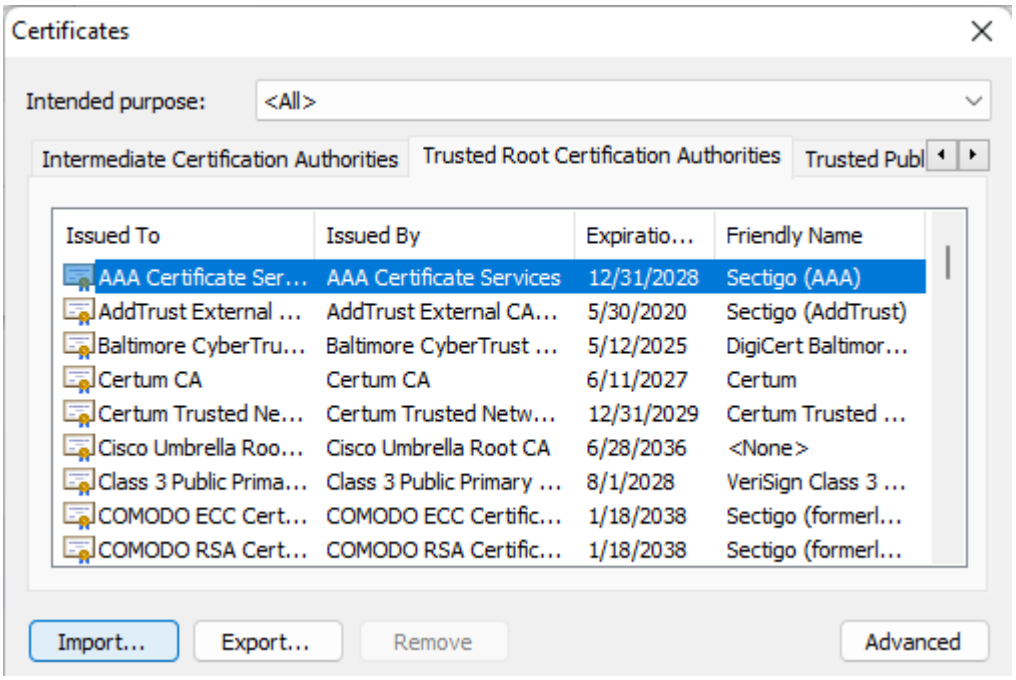
d) In the Security Window scroll down and click on the “Manage device certificates”.



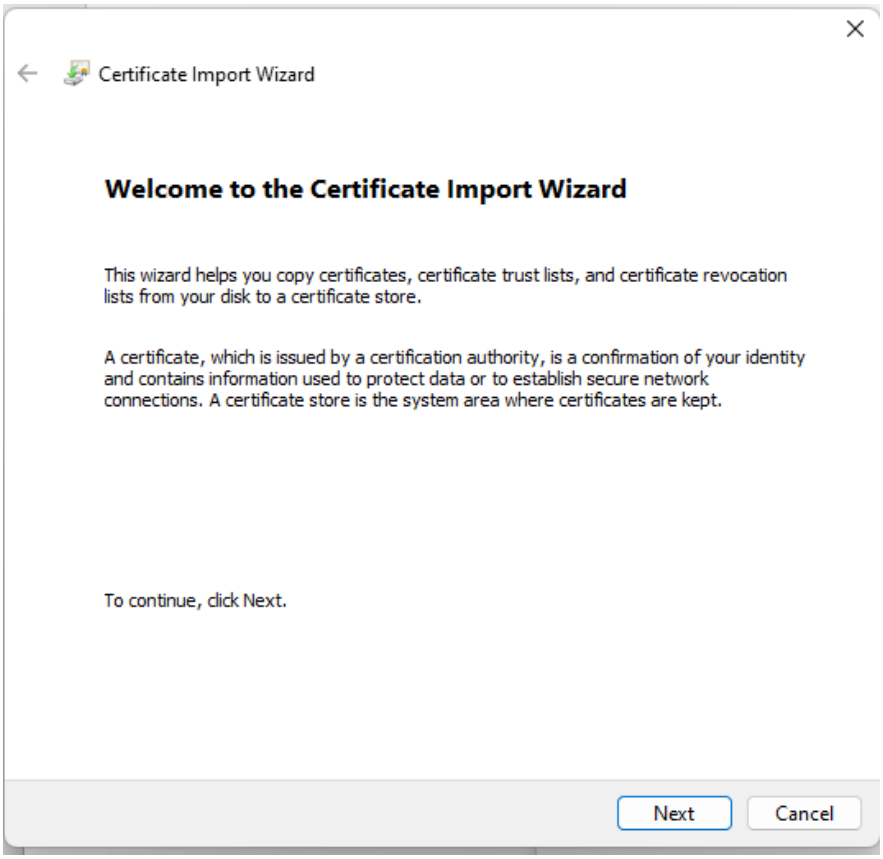
e) In the Certificates Window select the "Trusted Root Certification Authorities" tab.



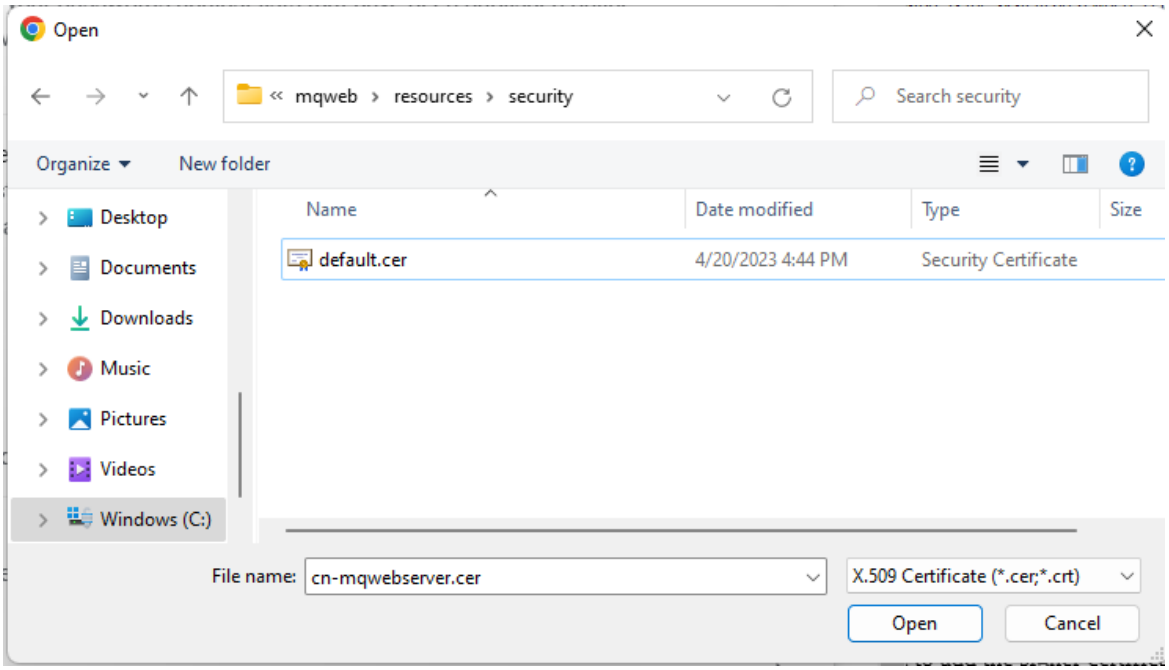
f) Click on "Import" and use the "Certificate Import Wizard" to browse to the location of the public.cer file and select it and click on Open.



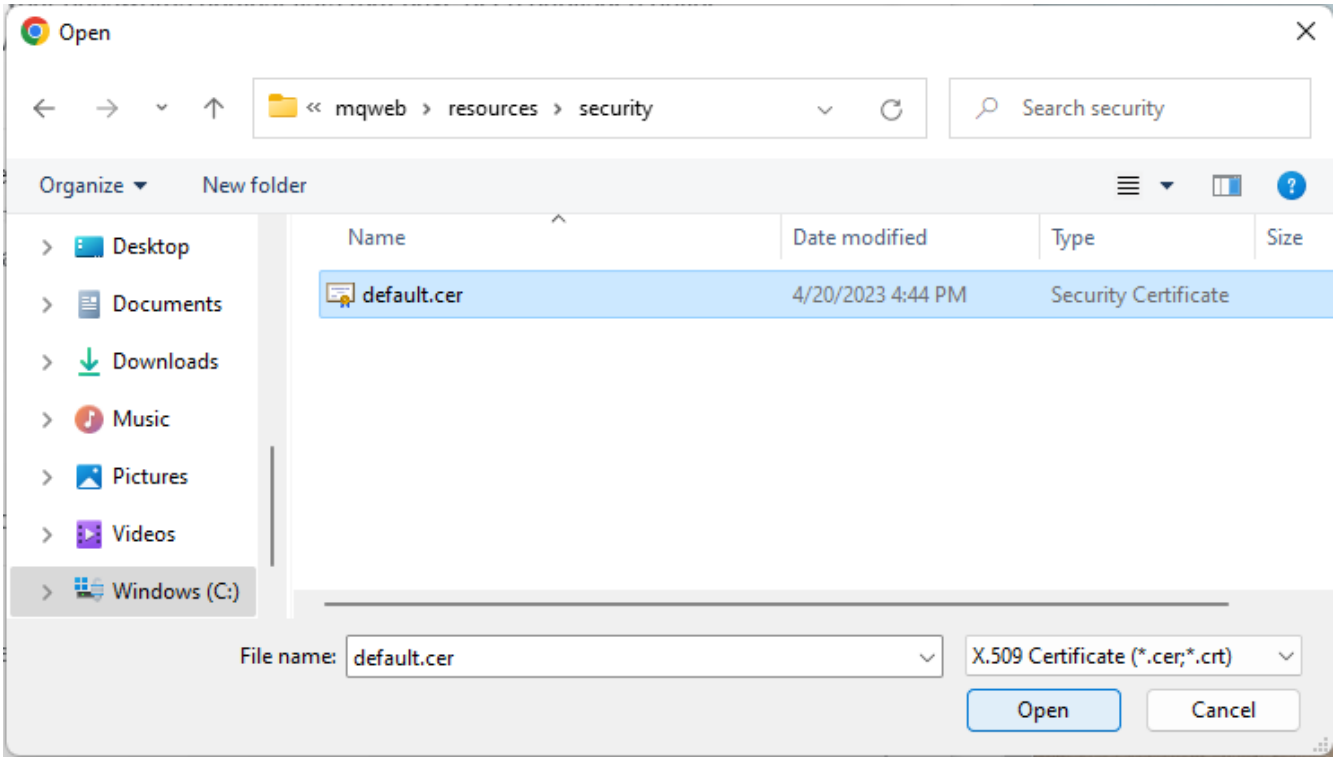
g) Press Next.



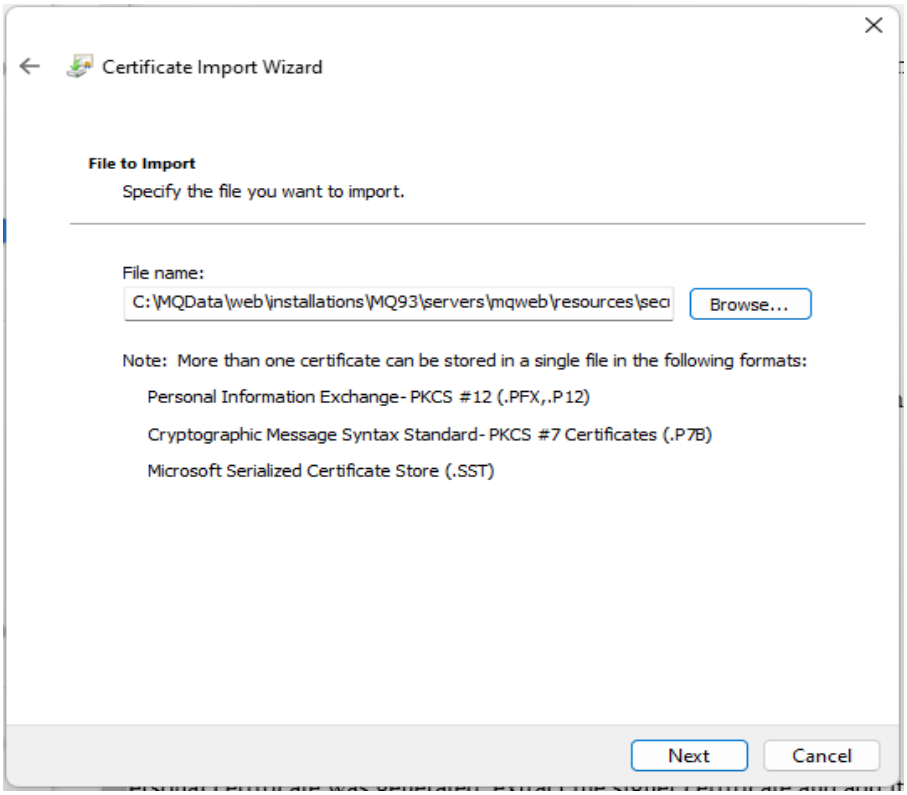
h) Press the “Browse” button and browse the File Explorer for the default.cer root signer certificate.



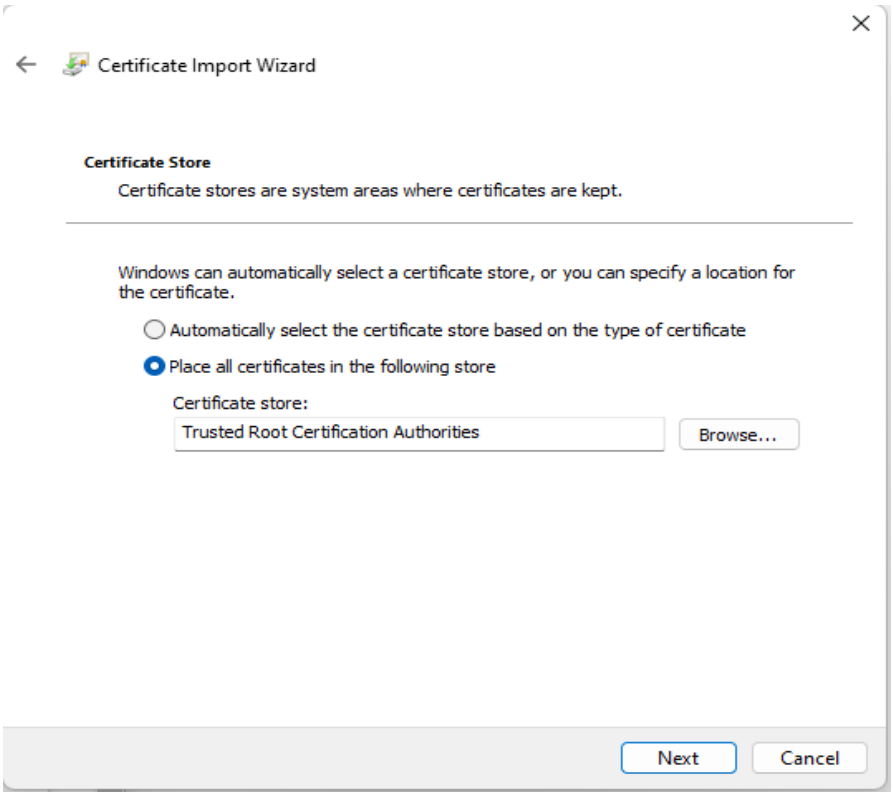
i) Select the default.cer file and press the “Opend” button to add the signer certificate into the browser's key repository.



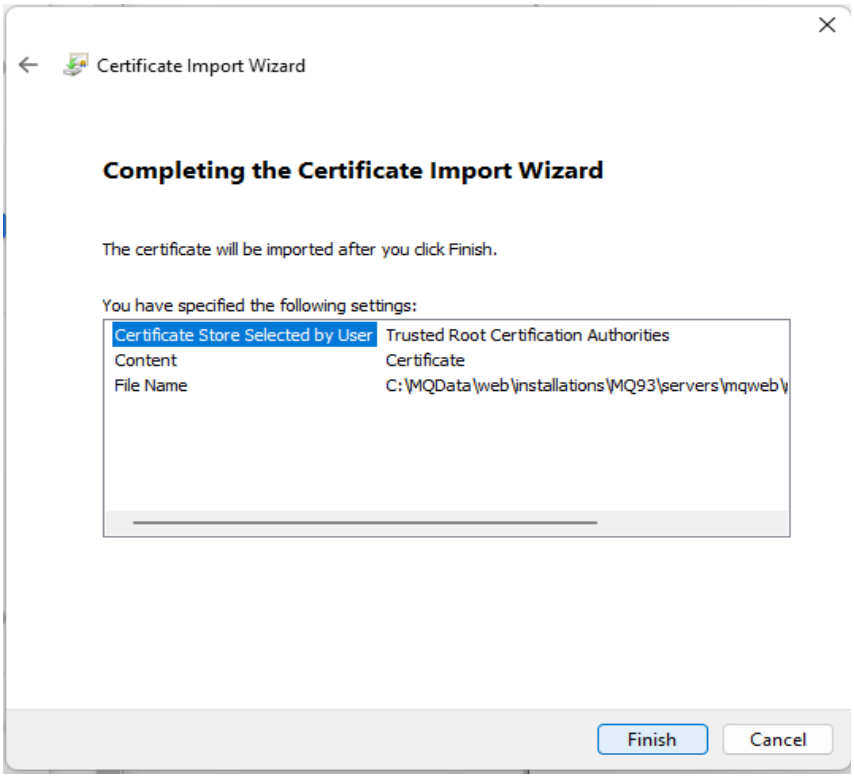
j) Press on the “Next” Button.



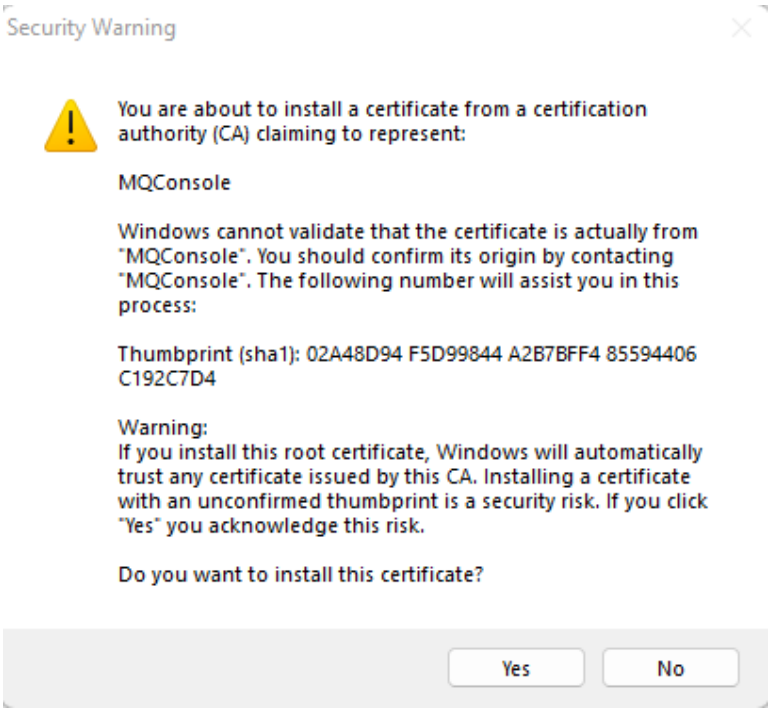
k) Press on the “Next” Button.



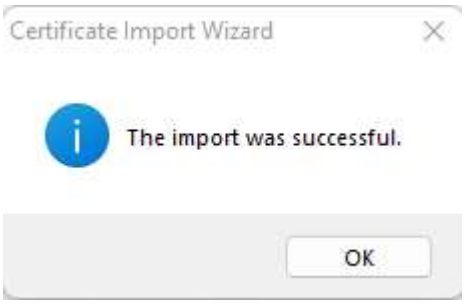
l) Press the “Finish” Button to add the certificate to the Trusted Root key ring.



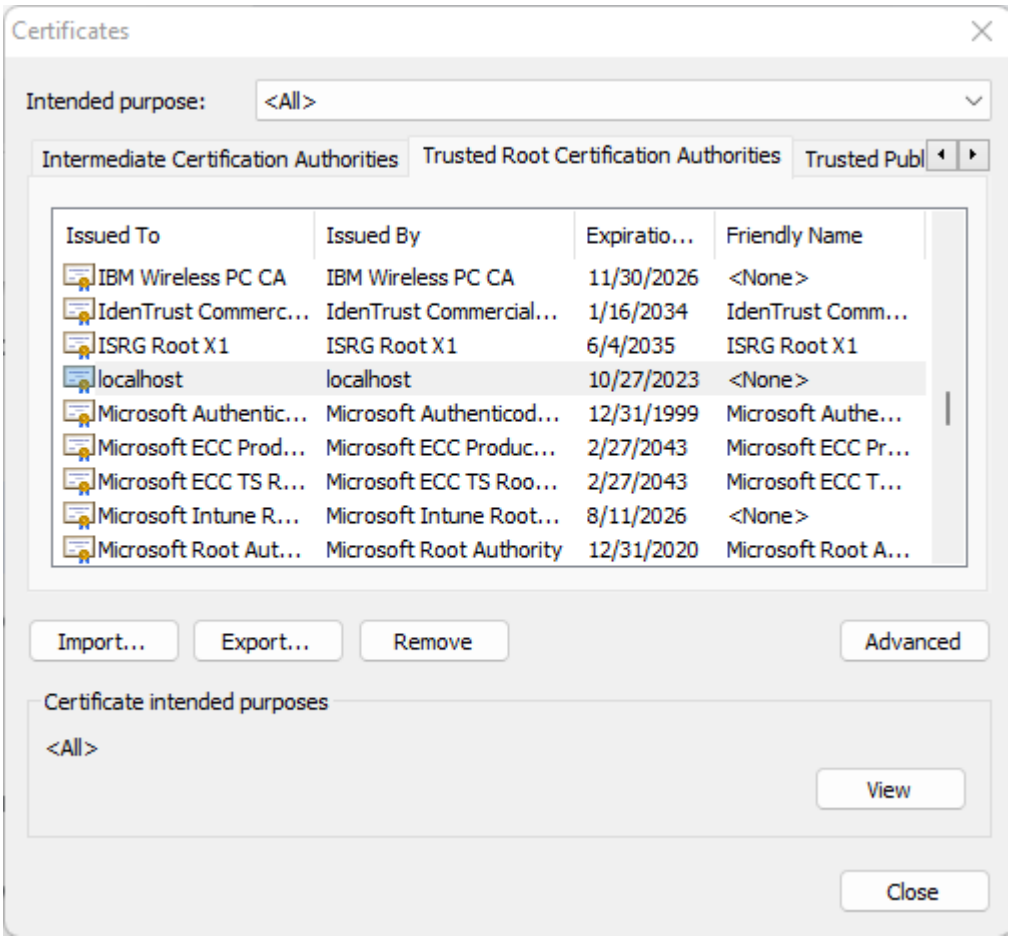
m) A “Security Warning” window will come up, press the “Yes” button.



n) A small window will be displayed informing you the certificate was imported successfully, Press the “OK” button.



o) In the “Trusted Root Certification Authorities” windows scroll down to a certificate called localhost. This is your trusted root signer certificate for the MQ Web Servers personal certificate called default.



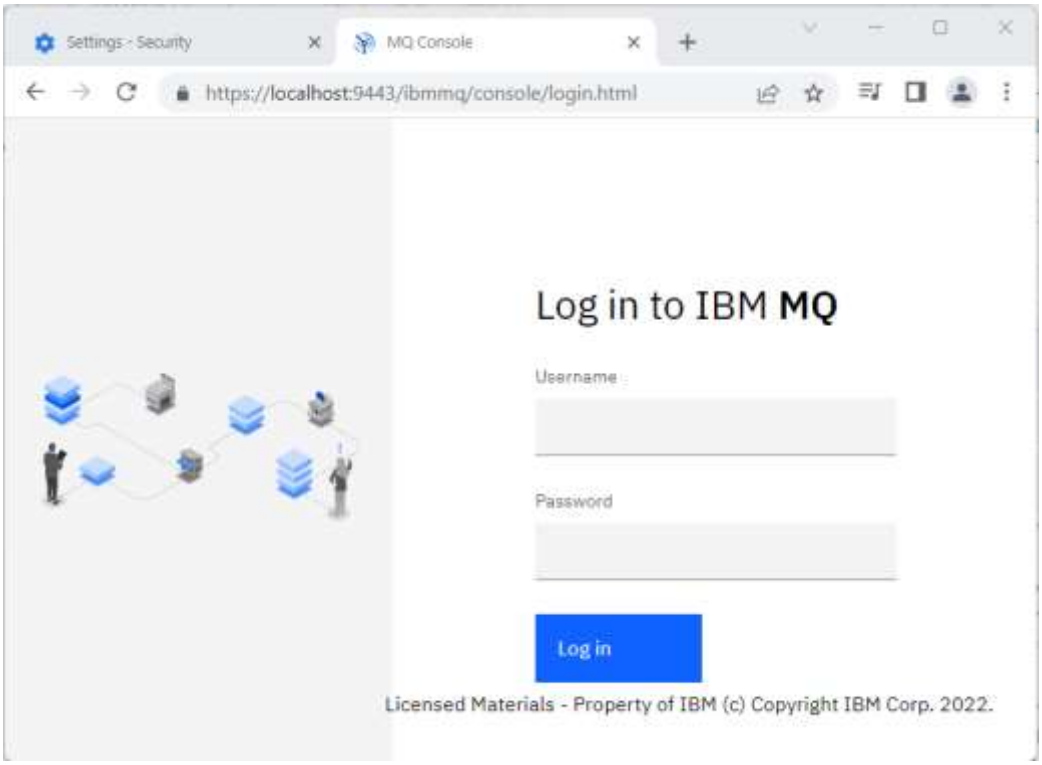
8. From step 4 paste the address to access MQ Console into your browser and press the “Enter” key.

For example: https://localhost:9443/ibmmq/console/

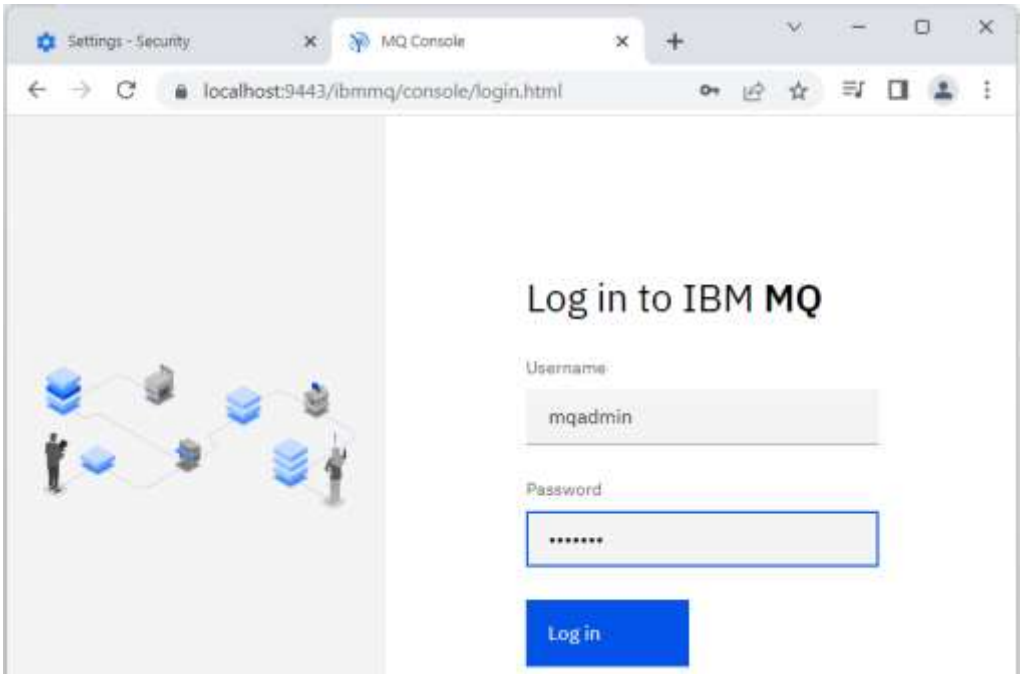
9. Login to the MQ Console using the default administrator's userId/password:

Username: mqadmin Password: mqadmin

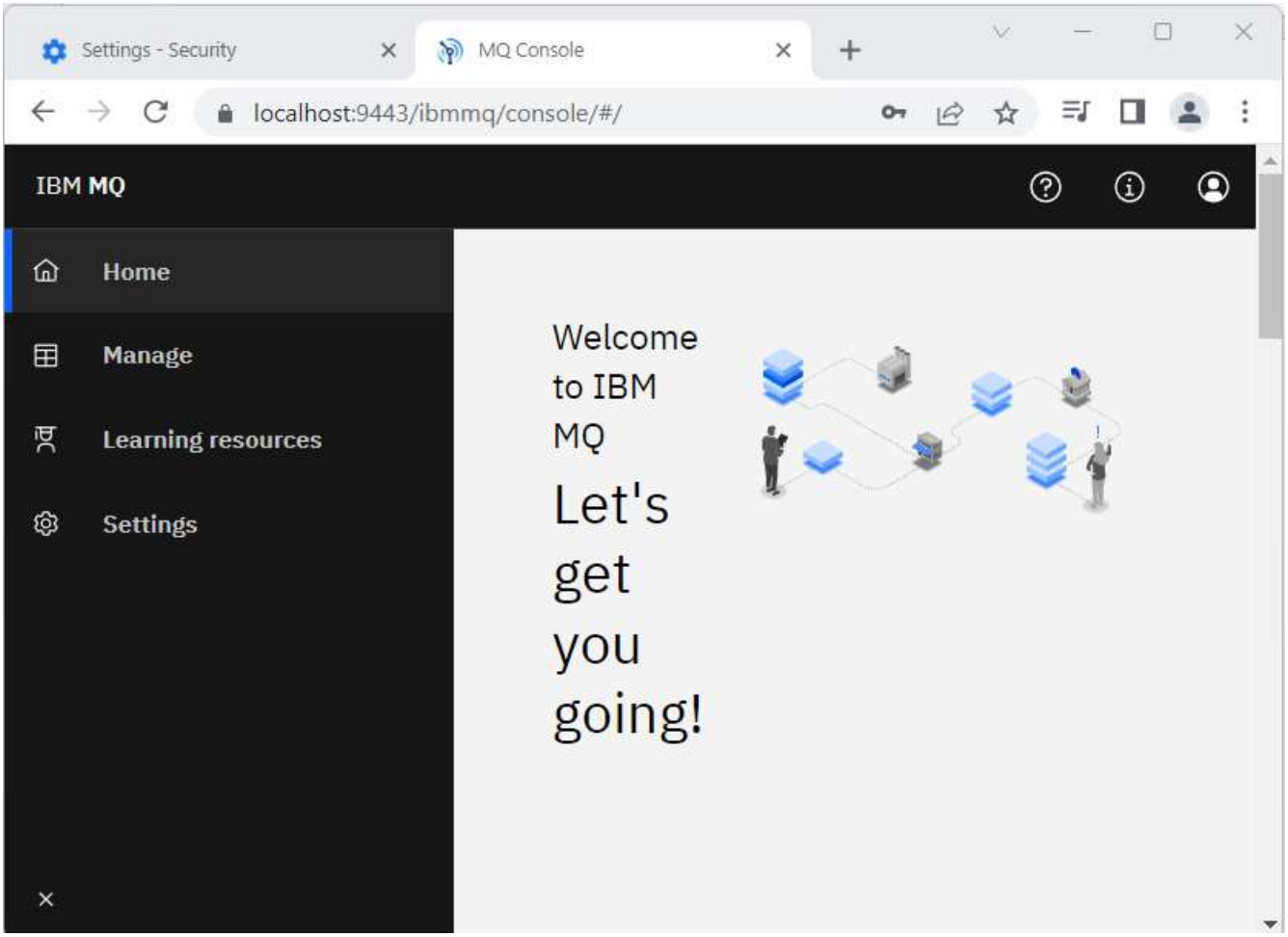
a) Confirm that your connection is secured by looking for the lock symbol on the left hand side.



b) After entering the Username mqadmin and Password admin, press the “Log in” button.



c) You are now logged into the MQ Console Home.



10. Configure the MQ Web Server to accept remote connections:

By default, the MQ Console is accessible only from the same host on which the mqweb server runs. Therefore, to enable remote connections to the MQ Web Server enter the following command before starting the mqweb server.

setmqweb properties -k httpHost -v hostname or IP Address

Where hostname specifies the IP address, domain name server (DNS) host name with domain name suffix, or the DNS host name of the server where IBM MQ is installed.
Use an asterisk, *, in double quotation marks, to specify all available network interfaces, as shown in the following example:

setmqweb properties -k httpHost -v "*"

11. Browser Requirements to allow the MQ Console to connect remote to the MQ Web Server.
In order to use an https connection, Microsoft Edge and Chrome would only allow the connection if a new MQ web server personal certificate were generated with its hostname or ip address in the Common Name (CN) field or use the Subject Alternative Names (SAN).

12. Creating a new self-signed certificate using a full hostname or IP Address.

Below are the runmqckm commands to create personal certificates using the CN or the SAN.

runmqckm -cert -create -label default -db key.jks -pw password -dn "CN=10.50.20.127,O=Messaging,C=US" -size 2048 -sig_alg SHA256WithRSA

or

runmqckm -cert -create -label MQWebServerCert -db key.jks -pw password -dn "CN=MQConsole,O=Messaging,C=US" -san_ipaddr 10.50.20.127-size 2048 -sig_alg SHA256WithRSA

13. Extracting the root signer certificate from the newly generated self-signed certificate.

Since a new self-signed personal certificate was generated, extract the signer certificate and add it to the browser's key repository as shown in steps 7-8.

runmqckm -cert -extract -label default -db key.jks -pw password

NOTE:
If you keep the original certificate in the key repository, rename it so that you can use "default" as your new certificate's label (name).

14. Restart your MQ Web Server so that the new certificate is used in the connection.
endmqweb and then strmqweb

15. Make sure the values set in your CN or SAN certificate distinguished name property(full hostname or ip address) is used to configure your MQ Web Console https connection. For example:

a. You stopped the MQ Web Server and restarted after the certificate change.
b. When you display the MQ Web Server address you receive the following output:
    a. https://hostname.Company.com:9443/ibmmq/console/
c. However, you configured the certificate with a SAN value of 10.50.20.127.
    a. Modify the https address to: https://10.50.20.127:9443/ibmmq/console/

NOTE: If you do not do this, Chrome will not consider this a secure connection because the full hostname value is not what was configured for your CN or SAN value. They both MUST match.

+++ end +++