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 <u>https://www.ibm.com/products/mq/support</u> 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_mgwebuser xml file and then rename the basic_registry xml file to

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 ".



0 × Settings - Privacy and security × + C
 Chrome chrome://settings/privacy ÷ \rightarrow A. -=1 ÷ Settings Q Search settings Your browser is managed by your organization You and Google . Safety check Autofill Ê Privacy and security ø Ø Chrome can help keep you safe from data breaches, bad extensions, and more Check now Performance O 680 Appearance Privacy and security 9 Search engine Clear browsing data 盲 Clear history, cookies, cache, and more Default browser Cookies and other site data (1) On startup ¢b . Third-party cookies are blocked in incognito mode. Languages Security Ø Safe Browsing (protection from dangerous sites) and other security settings. Downloads +

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



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

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

Certificates					×
Intended p	urpose: </td <td>\ll></td> <td></td> <td></td> <td>~</td>	\ll>			~
Personal	Other People	Intermediate Certification A	uthorities T	Frusted Root Certification	• •
Issued	То	Issued By	Expiratio	. Friendly Name	
📑 e30	52ce0-3218-4b.	IBM VPN PC CA	7/18/2024	IBM VPN PC CA	
	52ce0-3218-4b. -12-1-13281945	IBM Wireless PC CA G2 S-1-12-1-1328194585	7/18/2025 7/18/2052	i <none> ! <none></none></none>	

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.

uthorities Trusted Root Ce	ertification Aut	horities Trusted Publ
Issued By	Expiratio	Friendly Name
AAA Certificate Services	12/31/2028	Sectigo (AAA)
AddTrust External CA	5/30/2020	Sectigo (AddTrust)
Baltimore CyberTrust	5/12/2025	DigiCert Baltimor
Certum CA	6/11/2027	Certum
Certum Trusted Netw	12/31/2029	Certum Trusted
Cisco Umbrella Root CA	6/28/2036	<none></none>
Class 3 Public Primary	8/1/2028	VeriSign Class 3
COMODO ECC Certific	1/18/2038	Sectigo (formerl
	Ithorities Trusted Root Constraints Trusted Root Constraints AAA Certificate Services AddTrust External CA Baltimore CyberTrust Certum CA Certum Trusted Netw Cisco Umbrella Root CA Class 3 Public Primary	Ithorities Trusted Root Certification Aut Issued By Expiratio AAA Certificate Services 12/31/2028 AddTrust External CA 5/30/2020 Baltimore CyberTrust 5/12/2025 Certum CA 6/11/2027 Certum Trusted Netw 12/31/2029 Cisco Umbrella Root CA 6/28/2036 Class 3 Public Primary 8/1/2028

g) Press Next.

-	Certificate Import Wizard	×
	Welcome to the Certificate Import Wizard	
	This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.	
	A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.	
	To continue, dick Next.	
	Next Cance	4

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

7

💿 Open				×
\leftrightarrow \rightarrow \checkmark \uparrow	mqweb > resources > security	~ C ×	O Search security	
Organize 🔻 New folder			≣ ▼ 🔳	?
> 🛄 Desktop	Name	Date modified	Туре	Size
> 📑 Documents	🚽 default.cer	4/20/2023 4:44 PM	Security Certificate	
> 🛓 Downloads				
> 🕖 Music				
> 🔀 Pictures				
> 🔀 Videos				
> 🖳 Windows (C:)				
File name:	cn-mqwebserver.cer	~ X.	.509 Certificate (*.cer;*.crt)	~
			Open Cancel	

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

Open			×
$\leftrightarrow \rightarrow \cdot \cdot \uparrow$	mqweb > resources > security	~ C _> s	earch security
Organize 🔻 New folder			≣ ▾ 💷 😗
> 🛅 Desktop	Name	Date modified	Type Size
> 🔄 Documents	default.cer	4/20/2023 4:44 PM	Security Certificate
> 🛓 Downloads			
> 🕖 Music			
> 🔀 Pictures			
> 🚺 Videos			
> 🛄 Windows (C:)			
File name:	default.cer	√ X.509	Certificate (*.cer;*.crt) v Vpen Cancel

j) Press on the "Next" Button.

←	×
File to Import Specify the file you want to import.	
File name: C:\/MQData\/web\/installations\/MQ93\/servers\/mg/web\/resources\/seg	
Note: More than one certificate can be stored in a single file in the following formats:	
Personal Information Exchange- PKCS #12 (.PFX,.P12) Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)	Ì
Microsoft Serialized Certificate Store (.SST)	
Next Car	ncel

k) Press on the "Next" Button.

ertificate	Store				
Certifi	cate stores are s	system areas w	here certificat	es are kept.	
Windo the ce	ws can automati rtificate.	ically select a c	ertificate store	e, or you can spec	cify a location for
\circ	Automatically se	elect the certific	ate store base	ed on the type of	certificate
0	Place all certifica	ates in the follo	wing store		
	Certificate store	e:			
	Trusted Root	Certification Au	thorities		Browse

1) Press the "Finish" Button to add the certificate to the Trusted Root key ring.

- 🛃	Certificate Import Wizard	;
	Completing the Certif	icate Import Wizard
	The certificate will be imported afte	er you dick Finish.
	You have specified the following se	ettings:
	Certificate Store Selected by Use	Trusted Root Certification Authorities
	File Name	Certificate C:\MQData\web\installations\MQ93\servers\maweb\i
		Finish

9

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

Security W	/arning	×
	You are about to install a certificate from a certification authority (CA) claiming to represent:	
	MQConsole	
	Windows cannot validate that the certificate is actually from "MQConsole". You should confirm its origin by contacting "MQConsole". The following number will assist you in this process:	
	Thumbprint (sha1): 02A48D94 F5D99844 A2B7BFF4 85594406 C192C7D4	
	Warning: If you install this root certificate, Windows will automatically trust any certificate issued by this CA. Installing a certificate with an unconfirmed thumbprint is a security risk. If you click "Yes" you acknowledge this risk.	
	Do you want to install this certificate?	

Yes

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

No

Certificate Imp		\times
The	successful.	
	OK	

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.

ntended purpose: <al< th=""><th>> Authorities Trusted Root C</th><th>ertification Aut</th><th>horities T</th><th>rusted Publ</th><th>•</th></al<>	> Authorities Trusted Root C	ertification Aut	horities T	rusted Publ	•
Issued To IBM Wireless PC CA IBM Wireless PC CA ISRG Root X1 ISRG Root X1 ISRG Root X1 Microsoft Authentic Microsoft ECC Prod Microsoft ECC TS R Microsoft Intune R Microsoft Root Aut	Issued By IBM Wireless PC CA IdenTrust Commercial ISRG Root X1 localhost Microsoft Authenticod Microsoft ECC Produc Microsoft ECC TS Roo Microsoft Intune Root Microsoft Root Authority	Expiratio 11/30/2026 1/16/2034 6/4/2035 10/27/2023 12/31/1999 2/27/2043 2/27/2043 8/11/2026 12/31/2020	Friendly N <none> IdenTrusi ISRG Roo <none> Microsoft Microsoft <none> Microsoft</none></none></none>	Name t Comm ot X1 Authe ECC Pr ECC T Root A	
Import Export Certificate intended purpos <all></all>	. Remove			Advand	ed

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.

Settings - Security	🗙 🗿 MQ Console	×	+	. ~	-		×
← → C 🔹 https	://localhost:9443/ibmmq/i	console/login.html		16 ¢	≡l	0 3	I
<u>.</u>		Log in t	o IBN	4 MQ			
1 1	S 1	Password					
		Log in					
	Licensed f	Materials - Property	01 IBM (C)	Copyright	IBW C	orp. 202	2.

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

C is localhost:9443/ibmmq/console/login.html C is localhost:9443/ibmmq/console/login.html C is	🔹 Settings - Security 🗙 🔅 MQ Con	sole × + × - O)
<p< td=""><td>← → C a localhost:9443/ibmmq/con</td><td>iole/login.html 🗢 🖄 🕁 🖬 🛔</td></p<>	← → C a localhost:9443/ibmmq/con	iole/login.html 🗢 🖄 🕁 🖬 🛔
Username mqadmin Password		Log in to IBM MQ
Password		Username mqadmin
		Password



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:

 <u>https://hostname.Company.com:9443/ibmmq/console/</u>
- c. However, you configured the certificate with a SAN value of 10.50.20.127.
 - a. Modify the https address to: <u>https://10.50.20.127:9443/ibmmq/console/</u>

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.