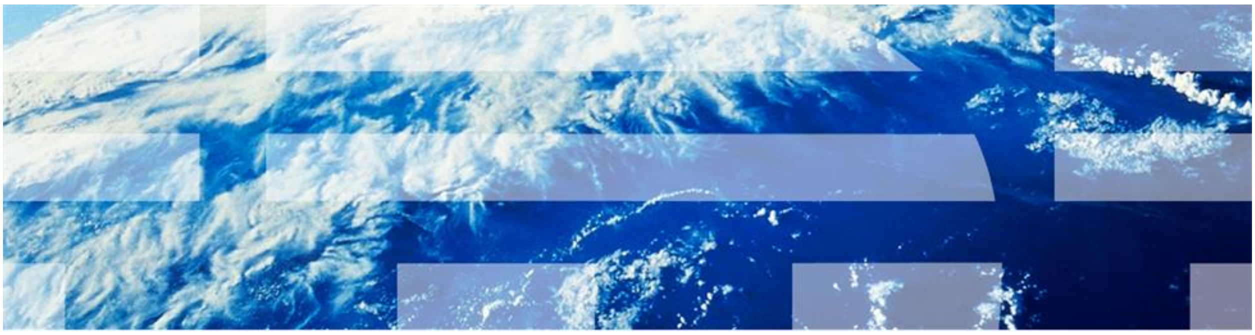
IBM Db2 Web Query for i

TLS Enablement



Updated April 18, 2023

TLS Enablement of IBM Db2 Web Query for i

It is strongly recommended to configure Web Query for Hypertext Transfer Protocol Secure (HTTPS) with the Transport Layer Security (TLS) protocol. TLS is a widely used security protocol for browsers and web servers. It is a successor version of the Secure Socket Layer (SSL) protocol. TLS establishes a secure connection between an end user's browser and a server by encrypting communications over the connection. Without this security, passwords and other sensitive data may be exposed.

1 Enable TLS for the HTTP Server

The IBM Web Administration for i console provides a TLS configuration wizard for HTTP servers. Use the wizard to enable TSL for Web Query's Apache server, WQLIB85. To access the console, go to https://*yourIBMi*:2001/HTTPAdmin. For detailed steps, refer to the IBM technote at https://www.ibm.com/support/pages/node/668113. Please note that the Web Query port for the HTTP server is 12331.

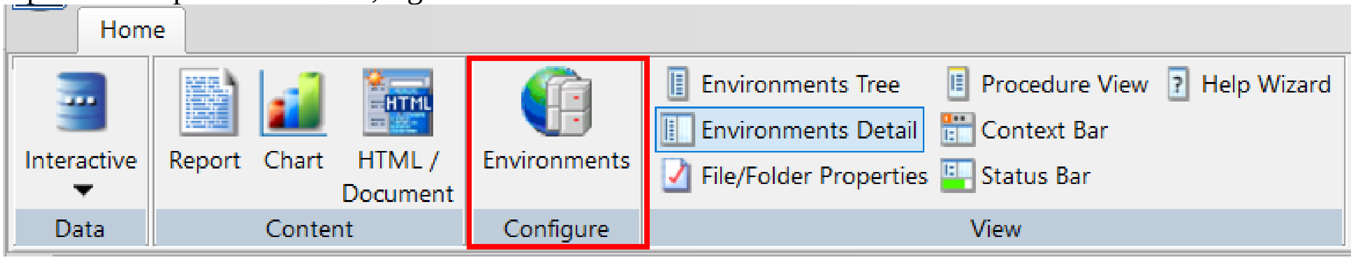
Once the HTTP server is enabled and restarted for TLS, the URL for the Web Query login screen is changed to https://<yourSystem>:12331/webquery. (http will no longer work.) The lock symbol in the URL search window confirms that the web server is using the secure protocol.

2 Enable TLS for Developer Workbench

To access Developer Workbench in the TLS environment, users will need to install the CA certificate on their PC before connecting to the Web Query server. This section describes how to connect to a Web Query server with Developer Workbench using an HTTPS connection.

1) Make sure Web Query is enabled for TLS and that you can access the Web Query portal with the URL https://*yourIBMi*:12331/webquery.

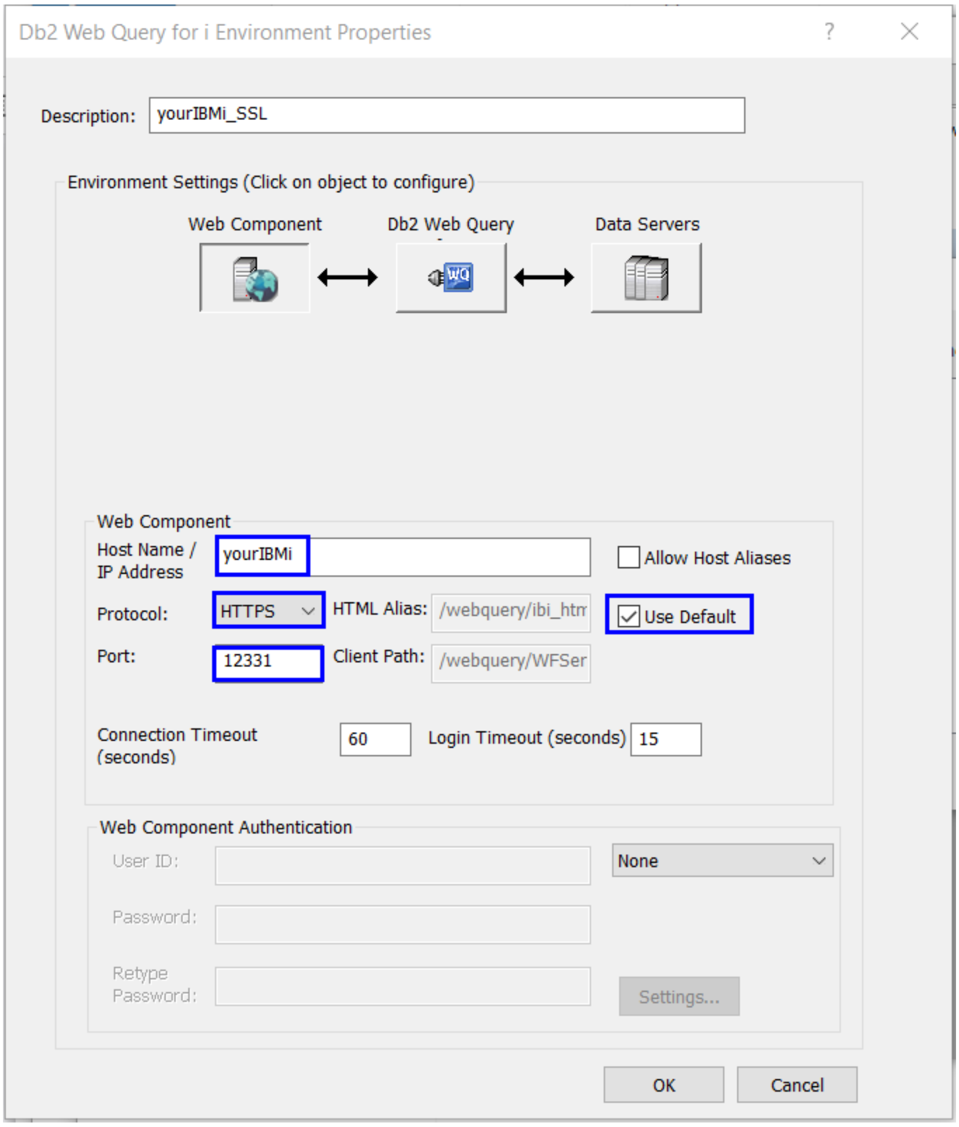
2) Open Developer Workbench, right click on the Environments and select Add.



3) In the Db2 Web Query for i Environment Properties panel shown below, enter the following and click OK.

Description: *This is the description of your connection*
Host Name/IP Address: *This is host name or IP address of the IBM i where Db2 Web Query is installed.*

Protocol: *Select HTTPS.*
Port: *Enter the Web Query port 12331.*
HTML Alias: *Check the Use Default box.*



Db2 Web Query for i Environment Properties

Description: yourIBMi_SSL

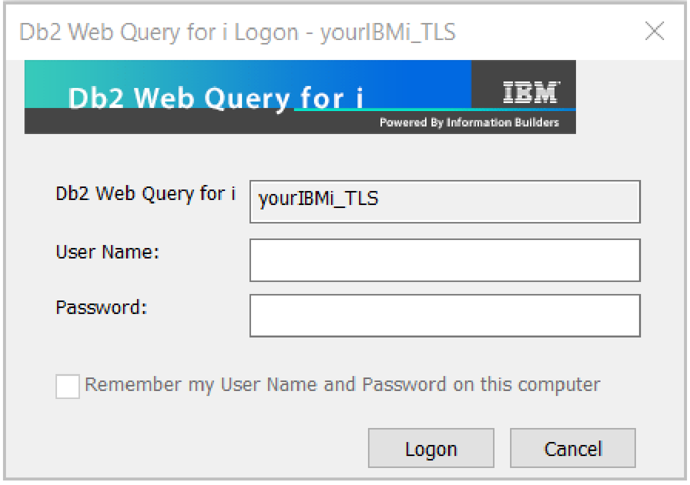
Environment Settings (Click on object to configure)

Web Component ⟷ Db2 Web Query ⟷ Data Servers

Web Component
Host Name / IP Address: yourIBMi
□ Allow Host Aliases
Protocol: HTTPS
HTML Alias: /webquery/ibi_htm
☑ Use Default
Port: 12331
Client Path: /webquery/WFSer
Connection Timeout (seconds): 60
Login Timeout (seconds): 15

Web Component Authentication
User ID:
Password:
Retype Password:
None

4) Enter your username and password and click Logon.



Db2 Web Query for i Logon - yourIBMi_TLS

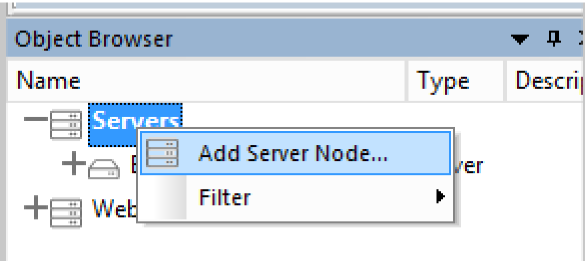
Db2 Web Query for i: yourIBMi_TLS
User Name:
Password:
□ Remember my User Name and Password on this computer

Developer Workbench will now use HTTPS secured by TLS.

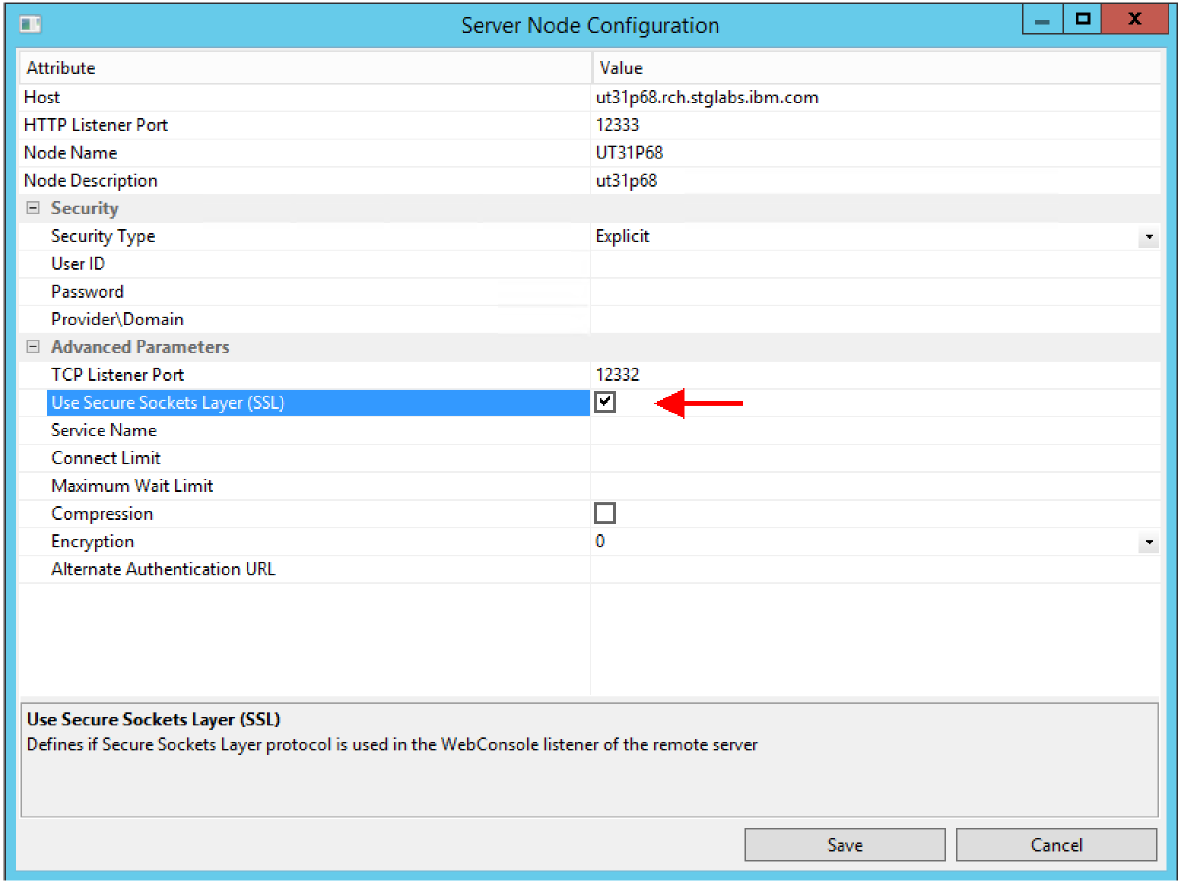
3 Enable TLS for the Data Management Console

The Data Management Console (DMC) installs along with the Developer Workbench client on a Windows PC. To access the Data Management Console (DMC) with TLS enabled, users will need to install the CA certificate on their PC before connecting to the Web Query server. To configure the server node connection to connect to the server using HTTPS, follow these steps.

1.Right-click on Servers and select Add Server Node.



2.On the Server Node Configuration panel, expand Advanced Parameters, and check the box for Use Secure Sockets Layer (SSL).



Attribute	Value
Host	ut31p68.rch.stglabs.ibm.com
HTTP Listener Port	12333
Node Name	UT31P68
Node Description	ut31p68
⊟ Security	
Security Type	Explicit
User ID	
Password	
Provider\Domain	
⊟ Advanced Parameters	
TCP Listener Port	12332
Use Secure Sockets Layer (SSL)	☑
Service Name	
Connect Limit	
Maximum Wait Limit	
Compression	□
Encryption	0
Alternate Authentication URL	

Use Secure Sockets Layer (SSL)
Defines if Secure Sockets Layer protocol is used in the WebConsole listener of the remote server

3.Click Save.

The DMC will now use HTTPS secured by TLS.

4 Enable TLS for JDBC-based Adapters

Web Query provides JDBC-based adapters for use with MySQL, Microsoft SQL Server, PostgresSQL, and other data sources. If you are using any of these optional adapters, then when enabling Web Query for TLS, it is also necessary to enable the adapter connection(s) for TLS.

To edit a connection, follow these steps.

1. From the Web Query hub, go to the Get Data panel.
2. Right click the adapter and select Show Connections.
3. Right click the connection and select Properties.

To enable a MySQL connection for TLS, edit the URL parameter to add the verifyServerCertificate, requireSSL, and useSSL properties, with useSSL last and no blank spaces, as follows:

jdbc:mysql://*host:port/*server?verifyServerCertificate=false&|requireSSL=true&|useSSL=true

To enable a Microsoft SQL Server connection for TLS, edit the URL parameter to add the encrypt and trustServerCertificate properties, as shown in the below example:

jdbc:sqlserver://*host:port*;encrypt=true;trustServerCertificate=true

Note that the properties added to the URL can vary, depending on how the Microsoft SQL Server is configured and depending on the JDBC driver's release level. For more information, refer to the JDBC driver properties at https://learn.microsoft.com/en-us/sql/connect/jdbc/setting-the-connection-properties?view=sql-server-ver16#properties.

PostgreSQL has several properties that can be used to enable SSL. For more information, refer to https://jdbc.postgresql.org/documentation/use/.

The generic JDBC adapter does not have a specific set of properties. Instead, it uses properties that are specific to the relational database management system (RDBMS) that the generic JDBC driver is connecting to. Refer to the RDBMS documentation to determine how to enable the connection for TLS.

5 Enable HTTP Strict Transport Security (HSTS)

HTTP Strict Transport Security (HSTS) is a browser security feature that prevents browsers from making unencrypted connections to a domain. That is, it enforces that all URL's use https:// instead of http://. When Web Query is TLS enabled, HSTS can be enabled for Web Query as follows:

1. End Web Query.
2. Edit /qibm/userdata/qwebqry/WQLIB85/wlp/usr/servers/WQLIB85/server.xml.
3. Add <webContainer addstrictransportsecurityheader="max-age=2;includeSubDomains"/>
4. Save the file.
5. Start Web Query.

Note that the maxage setting controls how long (in seconds) you want the browser to remember the HSTS header once it is seen. For example, when maxage=2, the browser will refuse to make unencrypted connections to the domain for two seconds.

6 Override TLS enforcement for Web Query startup

Beginning in release 2.4.0, Web Query startup will fail if the HTTP Apache server, WQLIB85, is not TLS or SSL enabled. Though not recommended, a system administrator can override the TLS enforcement at startup by updating the TLS_OVERRIDE setting in the Web Query configuration file QWQREPOS/QWQCONFIG.

Possible values for the TLS_OVERRIDE setting are:

- *DEFAULT: Default is *OFF.
- *OFF: Fail to start if TLS is disabled.
- *ON: Allow to start if TLS is disabled.

Below is an example SQL statement to configure Web Query to bypass the startup check and allow Web Query to run with TLS disabled.

```
UPDATE QWQREPOS/QWQCONFIG set VAL=’*ON' where PARM=‘TLS_OVERRIDE'
```