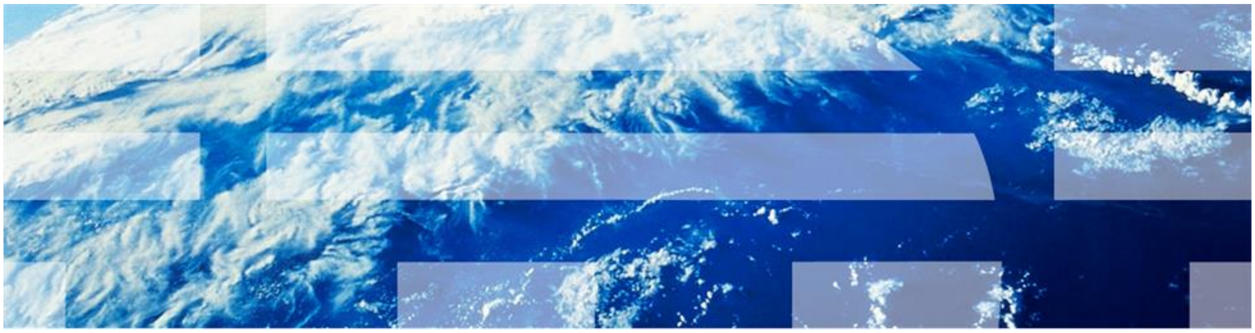
# IBM Db2 Web Query for i

## Deployment Guide / Best Practices

October 2022



# Preface

This document provides a summary of best practices for securing and deploying the IBM Db2 Web Query for i product. The intended readers of this document are system or security administrators, as well as Web Query administrators and developers. The recommendations in this guide will help to secure the Web Query environment, content, and application development.

# Secure the Environment

This section provides guidance to administrators to secure the underlying environment for a Web Query installation and application development. Administrators should incorporate these protections for the maximum level of security.

## *Enable TLS and HTTPS Protocols*

It is strongly recommended for Web Query to use Hypertext Transfer Protocol Secure (HTTPS) with the Transport Layer Security (TLS) protocol. TLS is a widely implemented security protocol for browsers and web servers. It is an improved, successor version of the Secure Socket Layer (SSL) protocol.

TLS establishes a secure connection between an end user's browser and the Web Query server. It adds confidentiality, integrity, and authenticity to communications by encrypting the data over the connection.

To enable Web Query to use HTTPS, an administrator must enable the web application server, WQLIB85, to use TLS. Instructions to configure HTTPS for the web application server, the Developer Workbench client, and the Spreadsheet Client, can be found at https://ibm.biz/db2wq-doc under the topic SSL Enablement.

## *Enable HTTP Strict Transport Security (HSTS)*

HTTP Strict Transport Security (HSTS) is a standard that prevents browsers from making unencrypted connections to a domain. It enforces that all URL's for the domain use https:// instead of http://. This ensures communications over the connection are encrypted and validated.

When the Web Query application server is enabled for TLS, HSTS can be configured to add an extra level of security to communications between users and the application server. HSTS can be configured as follows:

1. End Web Query.
2. Edit /qibm/userdata/qwebqry/WQLIB85/wlp/usr/servers/WQLIB85/server.xml.

3. Add `<webContainer addstricttransportsecurityheader=”max-age=xx;includeSubDomains”/>`
   where xx is a customizable number and 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.
4. Save the file.
5. Start Web Query.

It is recommended to use only secure connections between the client interfaces assigned to end users and the Web Query server. It’s also recommended to use HSTS.

## *Establish Firewalls*

To secure the Web Query infrastructure, it is recommended to establish web application firewalls and firewalls between all components of the network. Firewalls form barriers that help protect against malicious, external attacks.

## *Apply Software Updates*

It is best practice to stay current with the latest versions of the operating system, Web Query, and prerequisite IBM i products and features. Applying latest PTF levels helps ensure that the latest functional fixes and security patches are installed, and that the environment is protected from the latest security threats. For a list of the most recent Web Query PTFs, visit PTFs and On-going Service.

## *Perform Routine Backups*

It’s best practice before upgrading the operating system or before upgrading the Web Query release or group PTF level to perform a backup. It’s also a good idea to take routine backups to save any Web Query development work. This provides a means of recovery for unexpected events, but backups can also be useful to move Web Query to a different server or for initial setup of a high availability / replicated environment. A full system save does the trick but may be overkill for some situations.

To save the Web Query product, along with currently applied PTFs, use the Save License Program (SAVLICPGM) command. Separate commands must be issued for *BASE and each of the installed Web Query options. The SAVLICPGM will save the product libraries and the product directory. It does not save any user content, such as the reports, schedules, user registrations, or metadata.

A simple and best practice approach to save the user data is to use the Migrate Web Query (MIGWEBQRY) command. The MIGWEBQRY *SAVE operation bundles the repository library, the userdata directory, and the user licenses into one convenient save file. The MIGWEBQRY *RESTORE operation restores the saved information onto a target system and performs upgrades if the target system is at a higher Web Query level than what was saved. Noteworthy advantages of the MIGWEBQRY command (versus saving the library and directory manually) is that it handles the user licenses, and it handles the authorization lists that secure the metadata.

Another good practice for backing up or transferring Web Query content is to use the Change Management feature. It provides the capability to Export all or portions of the repository and metadata, and it conveniently saves it into a .zip file. The Change Management package can then be transferred or Imported later to recover the content.

References:

- For information on backing up an installation, refer to Backup, High-Availability, iASP, and Disaster Recovery.
- For information on MIGWEBQRY, refer to MIGWEBQRY command.
- For information on Change Management, refer to the Product Manual at Product Manual.

## Configure Server Settings

This section provides information for Web Query administrators or application developers to secure functions of the reporting server. Certain configurations may not be applicable to all environments, depending on requirements of the application and end users.

### *Use Secure FTP When Transferring Files*

The Report Broker tool provides scheduling and distribution capabilities for reports. One of the distribution options, FTP, allows report output to be transferred to a remote file on an FTP server. When using this feature, it's recommended to use the SSH File Transfer Protocol (SFTP), instead of the unsecure File Transfer Protocol (FTP), so that the data is encrypted as it is being sent. More information on configuring SFTP can be found at https://www.ibm.com/support/pages/node/1282276 under "Secure FTP".

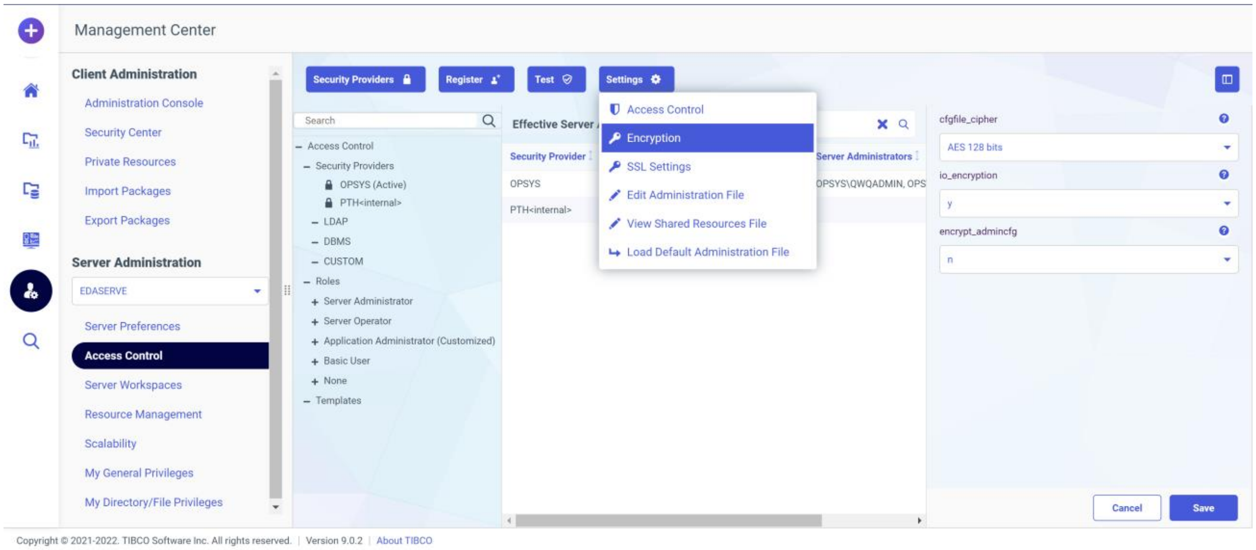
### *Encrypt Data at Rest*

The reporting server has capability to encrypt binary, alpha, and delimited HOLD files in the edatemp and foccache directories and data agent trace files. IBM i object security protects the files, so encrypting them serves as a double-down to prevent unauthorized users from opening and reading them in editors outside of the reporting server console or data management console. We recommend this protection be added as feasible, as it may compromise performance of the reporting server.

Encryption can be configured as follows:

1. Sign into the BI portal as a Web Query administrator.
2. Click the Gear icon and select Access Control.
3. Click Settings and select Encryption.
4. Set io_encryption to 'y'.

5. Click Save.



cfgfile_cipher: AES 128 bits

io_encryption: y

encrypt_admincfg: n

Note that after encryption the data agent trace files, tsxxx.trc and tsxxx.tro, will have the extensions .trce and .troe respectively.

## Configure Client Settings

The section addresses how to configure additional Web Query client settings to improve security based on the application requirements. The settings may not be applicable to all environments, depending on requirements of the application and end users.

### *Set the Session Timeout*

Reducing the time that sessions are open will reduce the time that they are vulnerable to unauthorized parties. Web Query Administrators can change the Session Timeout setting. It's located in the Administration Console, under Application Settings, and under BI Portal. It's best practice to replace the default value of 120 minutes with the shortest period that will accommodate the length of most sessions. For secure applications, a maximum timeout of 15 minutes is recommended.

For detailed steps to change the session timeout, go to https://www.ibm.com/support/pages/node/1282276 and see the topic Setting Limits.

## Manage User Access

User profiles, passwords, and object authorities are fundamental to IBM i security. Web Query builds on these fundamentals to provide security protection for the Web Query installation and to provide role-based user access to Web Query content.

## *Assign Web Query Administrators*

It is highly recommended to limit the number of users who are Web Query administrators and to assign the role only to users who have high system authorities already, such as a system or security administrator. Web Query administrators can do these tasks:

- Add or remove other licensed Web Query users
- Administer folder permissions for Web Query users
- Manage Web Query workspaces
- Configure Web Query
- Enable or disable diagnostic traces

## *Configure Mandatory Access Control (MAC)*

Mandatory Access Control (MAC) is a security strategy that restricts individual resource owners from granting or denying access to their resources. Instead, security is administered by a central authority, such as a system administrator. Users or owners cannot change the access of other users or objects.

It is highly recommended that MAC be enabled for Web Query. When enabled, the sign on password for the Web Query administrative profile, QWQADMIN, is removed so that users cannot sign onto the system or log into Web Query with that profile. Web Query administrators must then use their own ID to manage Web Query. This helps enforce a general security requirement in which each user should have only one sign-on and any operation should be accountable to only one person.

Instructions for enabling MAC can be found at https://ibm.biz/db2wq-doc under 'Mandatory Access Control'.

## *Restrict QWQADMIN profile*

The purpose of the Web Query administrative profile, QWQADMIN, is to be the *owner* of Web Query objects and the *runner* of Web Query server jobs. As mentioned previously, it is highly recommended to enable Mandatory Access Control (MAC) for Web Query and to ensure no password or sign-on capability is assigned to this profile. The QWQADMIN profile should not be shared and should not be granted special authorities.

## *Create Workspaces and Assign Folder Roles*

Web Query objects, such as reports, dashboards, schedules, and metadata, can be organized into workspaces, also referred to as folders or domains. When getting started with Web Query or creating a workspace, it's best practice to take a step back and think about who will develop or run reports in that folder. Consider what isolation is needed from other workspaces to ensure that only users who *need* access *have* access.

For each workspace, Web Query has six folder groups that represent a specific set of functions or roles. Those roles define what a user can do within a workspace, and consist of runner, analyst, developer, database administrator (DBA), scheduler, and administrator. These six groups (per workspace) are used to control what functions a user can perform on the objects in the folder. As is true when granting authorities to the underlying data sources for reports in that folder, it is an important security protection to only grant the minimum required workspace permission(s) to a user as required for their needs.

The run group assigns the minimum authority to a folder. Users in this group can only run reports in the respective folder; they cannot edit them or work with metadata. The developer group should be used for users who only create and edit reports and do not work with metadata. The administrator group should be used for users who can administrator other users within the context of that folder.  The folder roles are accumulative; to assign all the roles to a user for a particular folder, the user must be added separately to each group.

It is recommended that Web Query administrators not be added to folder roles.  Web Query administrators, by definition, have full access to all workspaces, so adding a Web Query administrator to a workspace role can be misleading and cause confusion.

There is one special workspace called Common that is provided out-of-box for all Web Query installations.  As its name implies, its content is intended to be common to (or shared by) all Web Query users.  Whether or not developers use this folder, it should not be deleted or renamed. There are dependencies on it in the Web Query repository.

Items in a workspace (such as reports or schedules) are stored in the Web Query repository that is a set of tables in the QWQREPOS library. Each workspace typically has a corresponding application directory in the IFS where the metadata associated with that workspace is stored. There is one special application called baseapp.  By default, it is shared by all Web Query users and by all workspaces.

In general, unless creating something that should truly be shared by all developers and used for all reports, such the image for a company logo, it's best practice not to use the Common workspace or baseapp. It's better instead to have a security strategy when organizing reports and administering user access.

More information on folder roles can be found in the Db2 Web Query Portal section, under the Security Center topic, in the Product Manual at http://ibm.biz/db2wq-prodman.

## *Enable Single Sign-On*

Enabling single sign-on (SSO) allows users to log on to their Windows workstation with a domain account, then automatically authenticate to the IBM i. This means when accessing Web Query from the browser, the login page is bypassed, and users are taken directly to the portal.  It's a user convenience.

Administrators who use the Configure Web Query SSO (CFGWQSSO) command to enable SSO should pay attention to the PWDEXP parameter. It controls what happens during an SSO sign-on if the user's IBM i password is expired. Though there's no recommendation either way to pass or fail the sign-on, it's best practice for administrators to be aware of the setting to make sure it meets their security or profile management requirements.

More information on how to configure SSO can be found at http://ibm.biz/db2wq-sso.

## *Secure the Data Source*

Web Query ensures only licensed users can log in and run reports. The Security Center allows an administrator to grant permissions to licensed users, controlling what folders a user has access to and what tasks the user can perform within those folders. It is, however, the system security administrator's responsibility to ensure the underlying data source for the reports is properly secured using IBM i and Db2 security controls. The data can be secured with object level authorities at the file and library levels. It can also be secured more granularly by Db2 at the row or column level. Again, it's best practice to grant only the minimum required authority to meet a user's right to know requirements.