Implementing Security in QW6

This document is intended to provide the QW Administrator with a detailed overview of the Security features available in QW6. For an overview tutorial of the features follow this link: https://qw6.busitech.com/managing-security/

There are two approaches to implementing Security in QW6.

- Windows Authentication + QW6 user permissions
- Standalone QW6 Security

Option 1 - Windows Authentication.

This method allows you to use the Windows Sign on Credentials to validate access to the QW6 Workstation and QW6 Admin modules.

Windows Authentication a definition:

> *Authentication is a process for verifying the identity of an object, service, or person. When you authenticate an object, the goal is to verify that the object is genuine. When you authenticate a service or person, the goal is to verify that the credentials presented are authentic.*

In QW6 terms it is the process of validating individual users who wishes to gain access to a workstation and in turn to QW6 applications.

The benefit of using Window Authentication is ease of maintaining User Id's and passwords. They can be managed at the Windows Administrator level and then employ all local criteria for setting and maintaining User Id's and passwords.

The QW6 Admin user would then add all the User Id's for users of QW6 to the QW6 Security database and then assign specific QW6 capabilities to individual users. There is no need to maintain passwords within the QW6 Database when Windows Authentication is employed.

Note: For data tracking purposes the Transaction Log file will identify each transaction with the Windows Authentication User Id.

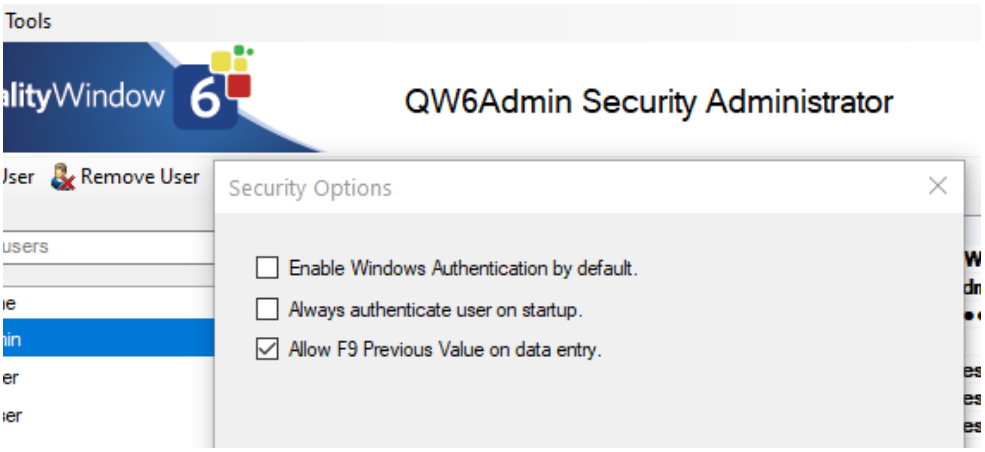
Enabling Windows Authentication in QW6

The first step is to have the Windows Administrator enable Windows Authentication on workstations using QW6.

- Select the QW6 Admin module Icon. 

- Select Security Administrator Icon 

Select Tools **Options**



This will open the QW6 global security settings window.

Enable Windows Authentication by default - when selected will enable Windows Authentication for QW6.

Always authenticate user on Startup - when selected will require a user to authenticate themselves when starting QW6 and that User Id will be used for data tracking purposes.

Allow F9 Previous Value on data entry – when selected allows the use of the F9 key to copy data from a previous record for individual variables.

The **+ QW6 user permissions** are common to both options and will be explained below.

Option 2 – Standalone QW6 Security

Using this method is like Windows Authentication for securing access to QW6 capabilities. The main difference is all User Id's and Passwords are created and managed in the QW6 Security Database.

Note: All passwords in the QW6 Security Database are encrypted and cannot be recovered if lost. New passwords can be assigned by the Security Administrator. It is very important to understand this also applies to the passwords assigned for access to the QW6Admin module and Security Administrator. It is recommended that two Users are assigned access to these two capabilities. In the case that access to QW6Admin is lost due to password issues, a user with who is a member of the Windows Administrator group can gain access to the QW6 Admin module. Contact Support@Busitech.com for instructions.

Creating the Administrator Users:

Note: An important first step in setting up QW6 Security is to create Admin user(s) to restrict access to several capabilities which regular users should not be given access to.

Adding new Users is a simple process just select the Add User at the top of the Security Administrator window.

Creating a new user is spearated into three sections:

- User Information
- User Permissions
- User Authentications

User Information:

This section is used first identify the user and also set access restrictions for QW6 capabilities.

- Full name of the User
- The User Name assigned here is the identification used in the audit trail logs of data as well as the Application Change logs when applications are modified in QW6Admin Applications Maintenance. If Window Authentication is used then the User Name must be the same user name used for Windows Authentication.

- Passwords once entered are encripted and can not be viewed. If Window Authentication is used leave blank.

The next group of setting are used to restrict access to QW6Admin functions used by Administrators. Users allowed to access these capabilities will all have access to the QWAdmin module but not have access to all the Admin functions. An example of this is a compnay may assign the Security Management to one user but not allow them to Manage Applications or access to the QWSpecmanager. It would be a good practise there is always two users with access to the Security Manager to insure continued access.

- Logon Domain – leave blank will use the default Domain for the workstation. Contact your Network Administrator if a different Domain is to be used.

- Access QWAdmin – should this user have access to the QW6Admin module – typically restricted to Admin type users only

- Manage Security – should this user be allowed to manage the security settings for users - typically restricted to Admin type users only.

- Manage Applications – provides access to the creation and maintenance of QW6 applications – typically restricted to Admin type users only.

- Access QWSpecManager – restrict access to the tool used to make non-structure changes to multiple QW6 applications such as Limits (Spec's, Control, Warning Target) as well as other values in the application templates. - typically restricted to Admin type users only.

- Password Expiry Date – if Windows Authentication is used leave this entry blank. If set, prompts user on expiry with a warning message to update their QW6 Security Password.

- Account Locked – set by an Admin user to lock the use of the User Id.

- Account Disabled – set by Admin user to temporarily suspend this User Id

- User Directory File – set by an Admin user to provide access to a defined list of a QW6 Applications. The use of a Directory File disables a users ability to navigate to other QW6 Applications on a Network. See video tutorial https://qw6.busitech.com/using-directory-files-in-qwadmin/

User Permissions:

The next section of the User Security settings relate to the ability to perform a function in a QW6 Application. Example: If the settings in a QW6 application set a restriction for deleting a record in the application then the current user will be prompted for their User Id and Password and verified they have that capability set in the Security database. If they do the function will be performed, if not, a message indicating they do not have that ability will be displayed. The transaction can either be cancelled or a user with the capability would have to authorize the action. All user Id's and actions performed would be recorded in the transaction log for that application.

- Read, Add, Edit, Insert, Copy, Delete – sets permissions for these individual transation capabilities.
- Allow Views – setting to No will restrict users from creating or changing Views in the Views Manager.
- Allow Signature – a feature not yet implemented
- Allow Previous Value – this would allow the user to use the F9 Previous value key on the Add screen.

User Authentications:

This section of the Security Settings is used to require users to enter their User Id's and passwords for performing the functions below. This function works with the User Permissions as well as the current User signed on.

Example: The current User signed in to QW6 is Laurie. Laurie selects to delete a record. In the security database Laurie has the permission to delete a record. So the delete can proceed. QW6 security then looks to the Authentication settings. If there is Authenticate Delete is Yes then the User will be prompted to Enter their User ID and Password. This validates that the signed in user is the one doing the delete. Authentication settings are very useful in a Team environment on a production line where not users have the same capabilities.

The User Id's that performed the task will be used to record the action in the transction log for that application.

Here is a table that outlines the different combination for Permissions and Authentication settings and how QW6 will respond.

TEMPLATE SECURITY	USER HAS PERMISSION	USER MUST AUTHENTICATE	RESULT
T,A,E,I,D,V	NO	YES	Prompt for user name and password. That second user must have permission to continue. This is the Manager Override feature. The Manager's credentials get sent to the transaction log.
T,A,E,I,D,V	YES	YES	Allow action to proceed ONLY after successful authentication. The authenticated user's name is sent to the transaction log.
T,A,E,I,D,V	YES	NO	Allow action to proceed without restriction. Prompt to authenticate if user is not already logged in.
T,A,E,I,D,V	NO	NO	Disallow action from proceeding. Permission denied error. This combination will disable a feature.