QualityWindow

The continuous improvement software

Quality Window Security – Admin Guide

Administration Guide

May 24, 2024

Table of Contents

Overview

This Security Administration guide is intended to help guide Quality Window Administrators in the deployment and configuration of the Quality Window security features. The security administrator console can be found in the Shared Data and Scripts section of QW6 Administrator.

Do we need Quality Window Security features enabled?

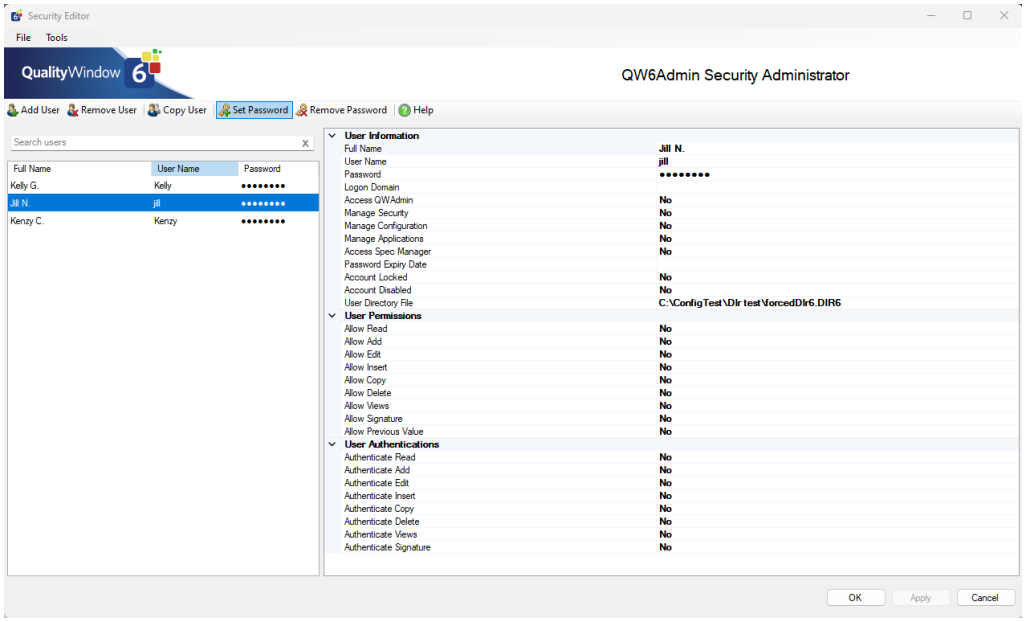
The Short answer is: **Yes. Busitech recommends you restrict access to the QW Admin console.**

Different organizations require different security stances. Busitech has ensured that Quality Window offers flexible and granular security capabilities that can meet any organization's needs. Due to the various needs of organizations Busitech's recommend recommended best practice is that QW Admin be limited to specific users as a minimum-security configuration.

If you feel that Quality Window would benefit from additional security features, please contact support@buistech.com with your idea.

Core Security Features

Quality Window provides the ability for administrators secure Quality Window data and Administration capabilities. This is done by configuring Quality Window to require users to authenticate and providing a robust governance model that provides granular user permissions and credential challenge configurations (user authentications).



Quality Window also provide two different authentication methods:

- Windows Authentication and Quality Window Security
- Standalone Quality Window Security

The main difference between these methods is where are user accounts and passwords managed: in Quality Window (standalone) or Windows Accounts (Local Windows Accounts or Domain/Active Directory accounts).

Configuring Quality Window Security

Quality Window Security provides options to ensure a good governance model for your organization. Below are the basic steps to implementing security in Quality Window:

1. Set up Shared Configuration
2. Review and Set Global Security Options.
3. Choose an authentication method.
4. Add Users accounts
5. Configure User security settings.
6. Configure QW Application Security.

Set up Shared Configuration

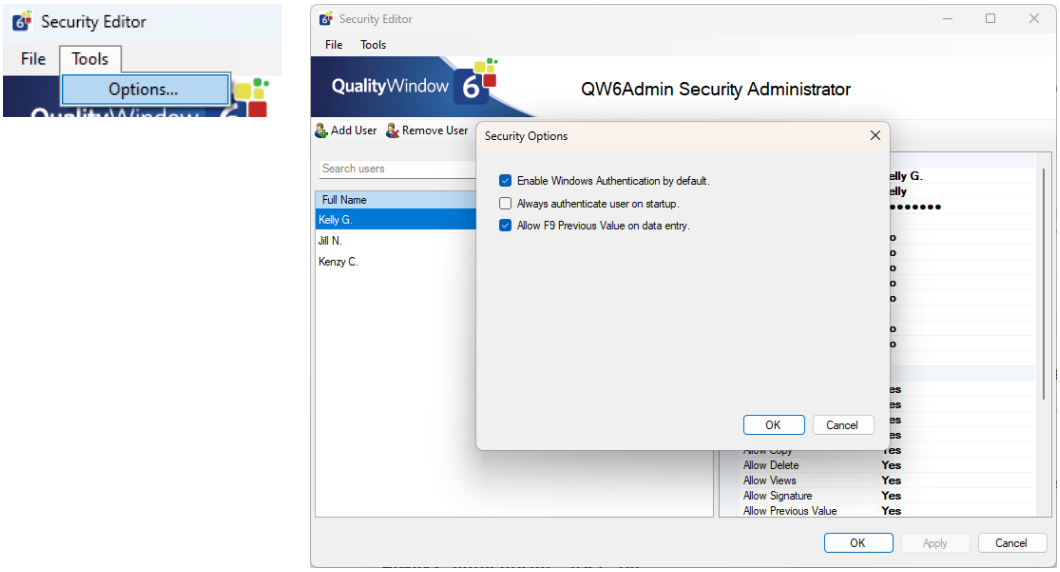
It is recommended that you first setup your shared configuration setup to ensure any configuration made following this guide will be applied to all client devices.

See our Shared Resources Tutorials for details:

1. Video Tutorial - Shared Resources Manager
2. PDF Guide - Distributing Shared Resource Files to all Workstations on a network

Global Security Options

Quality Window provides some global security options that can be applied to the Workstation without requiring individually set values in QW Applications. To access these settings, open the Security Administrator console and clock Tools -> Options menu.



Global Security Options

Global security Options settings Table:

Setting	Description
Enable Windows Authentication by default	When checked, all authentication prompts will be for windows authentication. See Choosing an Authentication Method for more details
Always Authenticate user on startup	When checked all users regardless of permissions or QW Application will be required to authenticate when accessing QW Workstation. *This does not apply to QW Admin.
Allow F9 Previous Value on Data Entry	When set to 'Yes' for any user, only users with setting set to 'Yes' will be able to Edit records in QW Applications.

Choosing an Authentication Method

As previously mentioned, there are two types of methods for authenticating users Windows Authentication or Quality Window Authentication. The difference between them is where user credentials (username & password) or originally defined and managed.

Quality Window Authentication

The default mode for Quality Window security where usernames and passwords and created and managed in Quality Window Security Administrator console and saved in Quality Window's security database (QWSecure.QWDB)

Windows Authentication

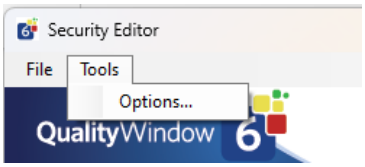
When this mode is enabled, the usernames and passwords are created and managed in windows or active directory. For the end user experience, when using windows authentication mode, users will need to enter the windows credentials when challenged for credentials as configured in user authentications. When password resets are required, or new user accounts created, this is managed in Windows users or Active directory if part of a company domain.

It should be noted that regardless of the Authentication method used, user accounts need to be defined in the Quality Window Security Administrator Console to apply user permissions and authentications configuration to each user.

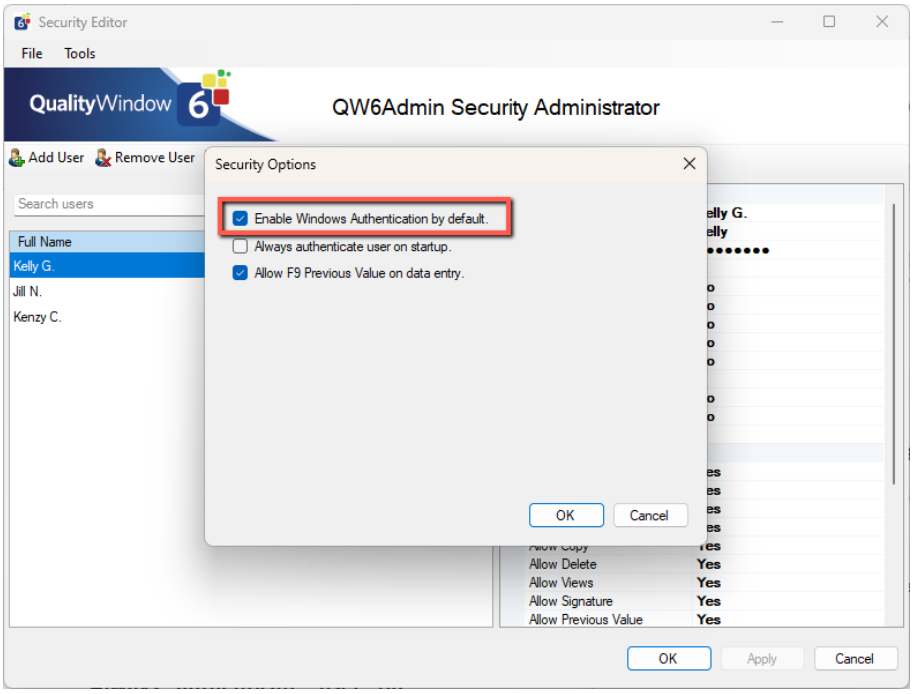
This mode does not currently support Microsoft Online Accounts (Live, Hotmail, etc..) only local or domain accounts.

Enabling Windows Authentication Method

To enable windows Authentication Method, navigate to the Security Administrator console in QW Administrator and click the Tools ➞ Options Menu.

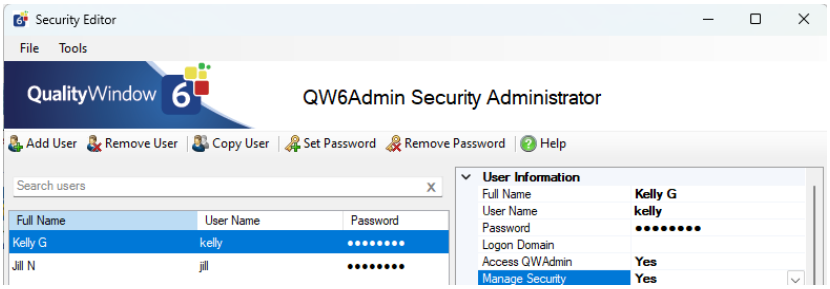


Next, ensure that the "Enable Windows Authentication by default." Checkbox is checked and click the OK button.



Managing Quality Window Users

User management is required for both authentication methods. This involves creating, configuring, deleting or copying user objects. If you are not using windows authentication, passwords must also be managed through the Security Administrator.



Creating Users

Click the add User button to add a user object and a new item will be added to the user list and you need to then provide a “Full Name” and a “User Name” to be able to save the user object. You may also configure other settings at this time. Details on each of the settings will be provided below. Click apply when completed.

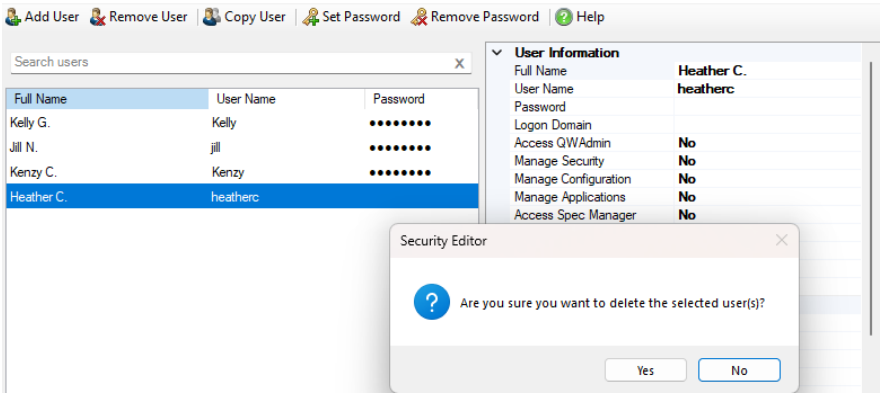
Creating users for windows authentication mode

When creating users for windows authentication mode, the User Name must match identically to the user name users would use to log into the device quality window is installed on. If users will log

onto a domain that is not the default domain assigned to the device, you will need to set the alternate domain in the Logon Domain field. Otherwise, the Logon Domain setting should not be used.

Deleting Users

To delete a user, select the user in the user list and click the remove user button a confirmation will be displayed. This action is irreversible once completed.



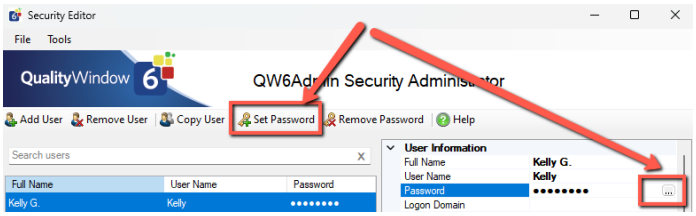
Copy User

Users can be copied, making it easy for user configurations to be replicated across multiple users. Click the copy user button and a new user object will be created with identical configuration except the following fields:

1. Full Name
2. User Name
3. Password

Setting a user's password

To set a user's password click the set password button on the toolbar or click the password … button in the property grid. Do not set passwords for users if using the windows authentication method.



Removing a user's password

The remove password feature on the toolbar allows administrators to remove a user's password when switching to windows authentication method.

Managing User configurations

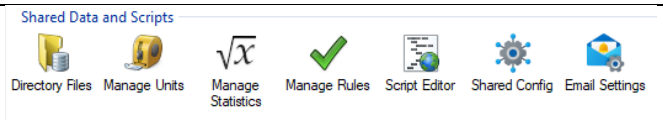
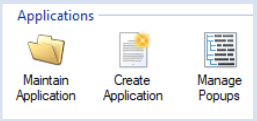
User's configurations are grouped in three sections. User information allows administrators to set user Administrator permissions, account, and credential settings. User Permissions allows administrators to configure workstation permissions while the user authentications section controls when are users challenged for credentials.

Configure User Information Settings

Below are the user information settings.

Note: With admin permissions found in user information settings, these security features remain disabled until a single user has been granted the permission. Said a different way, if no user has Access QW Admin permission set to Yes, then no user will require the permission to access the QW Admin.

Setting	Description
Full Name	User's Full Name, used to display in Workstation and Admin when showing who is currently logged in.
User Name	Username or user id for log in screen. Must be identical to username/user id as Windows credentials to match accounts.
Password	Only used for Quality Window Authentication method. Can only be set, cannot be read.
Logon Domain	Only used in Windows Authentication Method if domain is different from device default domain.
Access QW Admin	When set to 'Yes' for any user, only users with setting set to 'Yes' will be able to access QW Admin.
Manage Security	When set to 'Yes' for any user, only users with setting set to 'Yes' will be able to access Security Administrator. Also requires "Access QW Admin" permission. 
Manage Configuration	When set to 'Yes' for any user, only users with setting set to 'Yes' will be able to access the following QW Admin consoles: 1. Directory Files 2. Manage Units 3. Manage Statistics 4. Manage Rules 5. Script Editor (for global and folder level scripts) 6. Shared Configuration 7. Email Settings

	 Also requires "Access QW Admin" permission.
Manage Applications	When set to 'Yes' for any user, only users with setting set to 'Yes' will be able to access the following QW Admin consoles: 1. Manage Applications 2. Create Application 3. Manage Popups  Also requires "Access QW Admin" permission.
Access Spec Manager	When set to 'Yes' for any user, only users with setting set to 'Yes' and have the Manage Applications permission will be able to access the Spec Manager.  Also requires "Access QW Admin" permission.
Password Expiry Date	Set date for password expiry. Set in past to force password change for users. Currently Quality Window does not support setting a password change policy after X days.
Account Locked	When set to 'Yes' account is locked, and users cannot log in. This can be automatically set when user fails log in 3 times. Admins are required to unlock by setting value to 'No.'
Account Disabled	When set to 'Yes' account cannot be logged into.
User Directory File	Set user directory file which limits what applications a user can interact with on the open file dialog. See Tutorials on Directory files.

Configure User Permissions Settings

These permissions work with the specific security restrictions set at in the QW Application General Options tab- security options section. If a QW application has no security restrictions applied, then these permissions will not be applied. If on the other hand the QW Application has security restrictions applied, then for each of the applied restrictions a corresponding granted user permission is required. See Configuration QW Application Security for more details.

Below are the user permission settings that can be applied to users to govern the application data rights for users in QW Workstation when security restrictions are applied to a QW Application.

Setting	Description

Allow Read	When **Read** is restricted in a QW Application, only users with this setting set to 'Yes' will be able to Open, **View records and charts** in the QW Application.
Allow Add	When **Add** is restricted in a QW Application, only users with this setting set to 'Yes' will be able to **Add new records** in the QW Application.
Allow Edit	When **Edit** is restricted in a QW Application, only users with this setting set to 'Yes' will be able to **Edit existing records** in the QW Application.
Allow Insert	When **Insert** is restricted in a QW Application, only users with this setting set to 'Yes' will be able to **Insert new records** in the QW Application.
Allow Copy	When **Copy** is restricted in a QW Application, only users with this setting set to 'Yes' will be able to **Copy existing records** in the QW Application.
Allow Delete	When **Delete** is restricted in a QW Application, only users with this setting set to 'Yes' will be able to **Delete existing records** in the QW Application.
Allow Views	When **View** is restricted in a QW Application, only users with this setting set to 'Yes' will be able to **Edit or Create Views** in the QW Application.
Allow Previous Value	Overrides the global security option "Allow F9 Previous Value on data entry" (see Global Security Options)
Allow Signature	Currently Not used

Configure User Authentications Settings

User Authentications is a feature that forces a credential challenge regardless of the logged in user's permissions. This is useful when having devices shared amongst many users or in an open setting where many people could access the device.

These settings work with the existing QW Application security restrictions and the user permission settings. This means that user authentications/credential challenges will only be done if the QW Application has a companion security restriction and permission granted only if the credentials provided have permission to complete the requested task.

Setting	Description
Authenticate Read	When **Read** is restricted in a QW Application and this setting is set to 'Yes,' Users will be challenged for credentials every time a QW Application is opened.
Authenticate Add	When **Add** is restricted in a QW Application and this setting is set to 'Yes,' Users will be challenged for credentials every time an **Add Record** operation is initiated in the QW Application.

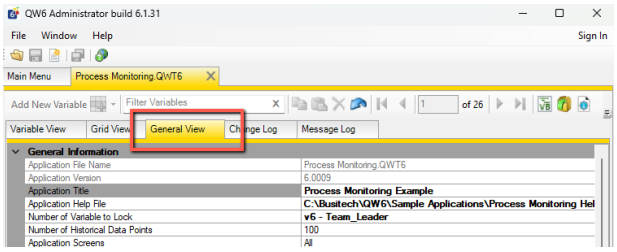
Authenticate Edit	When **Edit** is restricted in a QW Application and this setting is set to 'Yes,' Users will be challenged for credentials every time an **Edit Record** operation is initiated in the QW Application.
Authenticate Insert	When **Insert** is restricted in a QW Application and this setting is set to 'Yes,' Users will be challenged for credentials every time an **Insert Record** operation is initiated in the QW Application.
Authenticate Copy	When **Copy** is restricted in a QW Application and this setting is set to 'Yes,' Users will be challenged for credentials every time a **Copy Record** operation is initiated in the QW Application.
Authenticate Delete	When **Delete** is restricted in a QW Application and this setting is set to 'Yes,' Users will be challenged for credentials every time a **Delete Record** operation is initiated in the QW Application.
Authenticate Views	When **View** is restricted in a QW Application and this setting is set to 'Yes,' Users will be challenged for credentials every time a **New View or Edit View** operation is initiated in the QW Application.

Configuring QW Application Security Restrictions

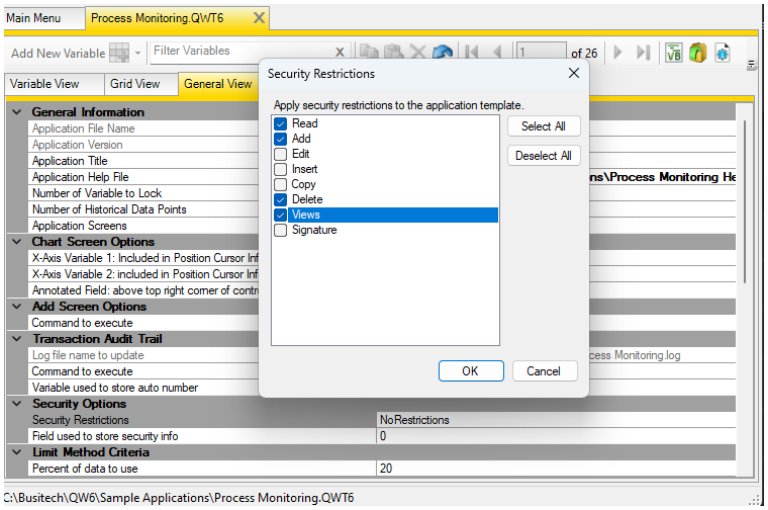
The last step to enabling security is to enable security restrictions on your QW Applications. Quality Window security is designed to be flexible and allows administrators to choose which applications need security and which do not. The default state of an QW Application is to not have security applied.

To enable security on a QW Application, open the QW Application in the Maintain Application console in QW Admin.

Next, click on the general View tab.



Then click the "…" button on the Security Restrictions Setting in the Security Options section of the General View tab.



Example Security Restriction in a QW Application.

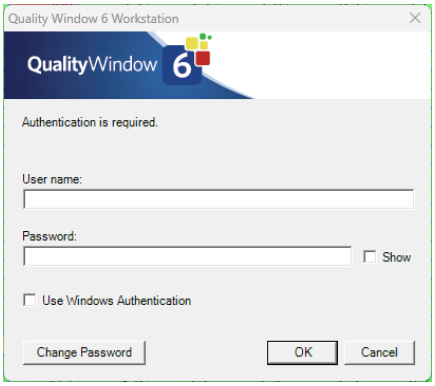
Select which Restrictions should be applied to the application and click ok then save the QW Application.

Repeat this process for each application you wish to have security restrictions applied to.

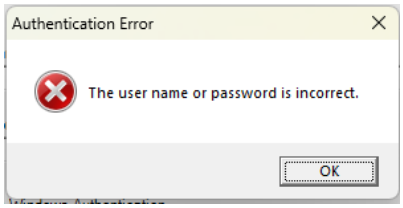
End User Security Experience

Authentication Screen

The Authentication screen or credentials screen allows users to provide their credentials (username and password), use Windows authentication method. If user credentials do not match, an error message will be displayed. This screen will be displayed anytime users initiate a sign in operation or try to complete a task that has been restricted by security configurations.



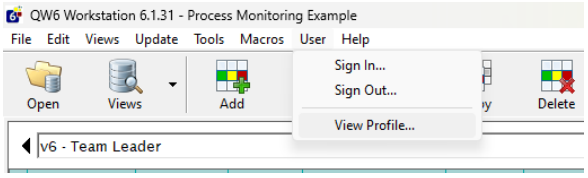
Sign in Dialog – Authentication



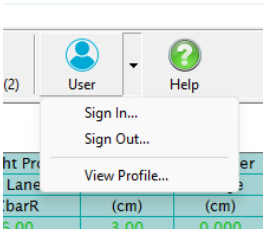
Error screen for incorrect credentials

Signing in/out on QW Workstation

Users can sign in, change users, sign out QW Workstation one of two ways if not forced due to security configuration which are the Tool bar or Menu bar.



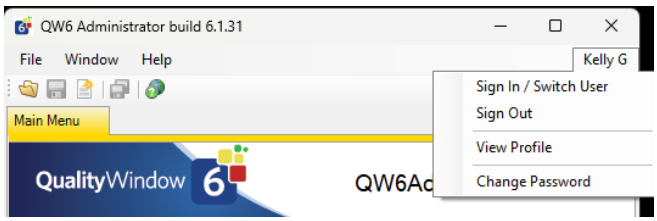
Menu bar user options



Tool bar user options

Signing in/out on QW Admin

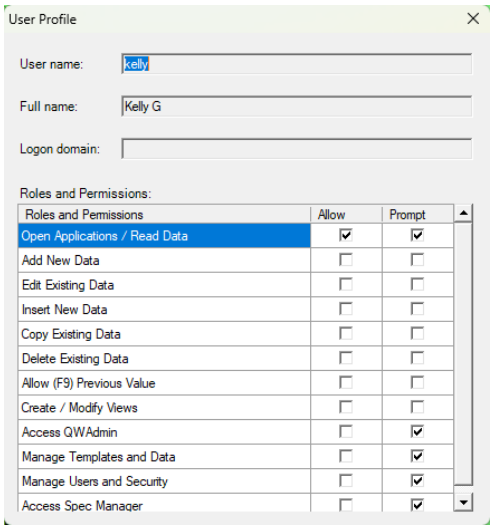
Administrators can sign in/out view profile by accessing the user menu in the top right of QW Admin.



User menu QW Admin

User Profile Screen

Users can view their own security restrictions by clicking 'View Profile…' on the menu or tool bar user menu items.



User profile screen

Support for other Authentication Features

Currently Quality Window does not support the following advanced authentications features:

- 2 Factor (2FA)
- Multi Factor (MFA)
- One Time Password (OTP)
- Windows Hello integration
- Microsoft Authentication Method with Microsoft Online Accounts (Hotmail, Live etc…)

If your organization want either of these capabilities, please send an email to support@busitech.com and share this feedback.

Troubleshooting

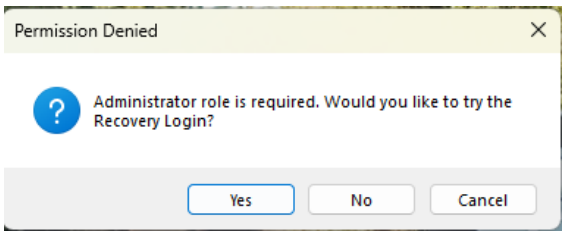
Below are common issues encountered by users and steps to troubleshoot the issue.

My user name and password is not working on 1 device while it works find on another device?

Validate your shared configuration settings, as the QWSecure.QWDB file is unique on the problem device. See Set up Shared Configuration section.

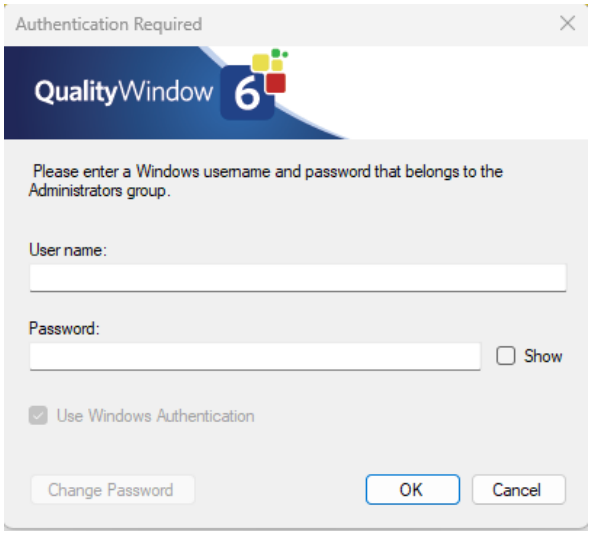
I cannot remember my Admin password and I am locked out of QW Admin how do I get access?

Typically, when this is the case administrators are presented with the following message.



Admin Recovery message

Clicking yes will allow you to attempt to log in using Windows Administrator Credentials. Enter your Windows credentials that are a member of the local administrator group and you will be granted access to QW Admin where you can update your passwords and/or security settings.



This will only work with local or active directory accounts. If you are using a Microsoft online account or do not remember your administrator credentials you will need to contact Busitech Support.