

QualityWindow

The continuous improvement software



Quality Window 6.1 in Regulated Environments

Product Controls and Supporting Capabilities

September 21, 2026

Table of Contents

Overview	3
Control Summary.....	3
Deployment and Data Control	3
Authentication and Access Control.....	3
Administrative Permissions	4
Application Permissions	4
Controlled Data Modification.....	4
Controlled Workflow Actions	5
Transaction Audit Trail	5
Administrative Change Audit Trail	6
Application Change Archives	6
Security Audit Logging.....	6
Backup and Recovery.....	7
Software Validation and Change Assessment.....	7
System Requirements	7
Use in Regulated Environments	8
Supporting Quality Window Documentation.....	8

Overview

Quality Window 6.1 (QW) provides security, access-control, audit-trail, data-control, and administrative capabilities that can support organizations operating in regulated manufacturing and quality environments.

This document summarizes the product controls available in current releases and identifies supporting Busitech documentation. It is intended to help quality, validation, IT, and security teams understand what QW provides when evaluating or operating Quality Window in a controlled environment.

Quality Window does not, by itself, make a customer implementation compliant with a specific regulation or create a validated system. Regulatory applicability, intended use, configuration, infrastructure, operating procedures, and validation activities remain specific to the organization using the software.

Control Summary

Control Area	Quality Window Capability
Deployment and data control	On-premises; customer controls infrastructure and data location.
Authentication	Quality Window or supported Windows authentication.
Access control	Administrative and application permissions with optional credential challenge.
Controlled data modification	Protected Variables and authorized override with audit logging.
Transaction audit trail	Add, Edit, Copy, Insert, and Delete history;
Security audit logging	User, permission, and authentication events. Security Setting updates.
Controlled workflow actions	Permission-based Alarm Acknowledgement. Protected (Read-only) variable override permissions.
Backup and recovery tools	Application backup and restore utilities.
Validation and change support	Build-specific validation documentation and release notes.

Deployment and Data Control

Quality Window is an on-premises application. Quality Window application data remains within the customer's environment by default, allowing the organization to manage the systems, storage, network access, backup, retention, and recovery controls that apply to its implementation.

Quality Window application data is primarily stored using [Quality Window proprietary application and data file formats](#) rather than a traditional relational database. Customers control the infrastructure on which Quality Window and its application data are deployed.

Authentication and Access Control

Quality Window provides a configurable security system for controlling access to administrative functions and application data. Two authentication approaches are supported:

Quality Window in Regulated Environments - Product Controls

- [Quality Window authentication](#), where usernames and passwords are managed within Quality Window Security Administrator.
- Windows authentication, using supported local Windows or domain/Active Directory accounts.

Regardless of authentication method, Quality Window user accounts are defined in Security Administrator so that permissions and authentication requirements can be applied to each user.

Administrative Permissions

Administrative permissions can restrict access to functions such as:

- QW Admin
- Security administration
- Application management
- Configuration management
- Specification management
- Tools and utilities

Application Permissions

Application-level security restrictions can be paired with user permissions for actions including:

- Read
- Add
- Edit
- Insert
- Copy
- Delete
- View management
- Alarm acknowledgement

When a restriction is enabled on a QW Application, the user must have the corresponding permission to perform the restricted action. Quality Window can also be configured to require a credential challenge when specified restricted actions are initiated.

Quality Window authentication also provides account controls including account lock and disable settings. Passwords managed by Quality Window can be set but are not displayed in readable form. Detailed authentication capabilities and current limitations are documented in the [Quality Window Security - Admin Guide](#).

Controlled Data Modification

Quality Window supports Protected Variables for values that should not normally be modified through routine data-entry operations.

Current QW releases also provide a [Protected Variable Override control](#). When the override capability is enabled, only users granted the corresponding permission can temporarily override a protected Variable, and the user must authenticate before the protected value can be edited. Override activity is recorded in both the Security Audit Log and Transaction Audit Trail.

Controlled Workflow Actions

Some Quality Window functions combine permissions, authentication, and audit logging to support controlled operational actions. Alarm Acknowledgement can be restricted to authorized users. Where configured, users without the required permission can be prompted for credentials from an authorized user before an alarm is acknowledged.

These controls allow an organization to [configure approval or acknowledgement responsibilities](#) without requiring the current workstation user to sign out and back in.

Transaction Audit Trail

Quality Window maintains a transaction audit trail for changes to application data. Beginning with QW 6.1.120, transaction audit logging is automatically enforced for applications and does not require an administrator to enable individual audit-log settings.

The transaction audit trail records application data operations including:

- Add
- Edit
- Copy
- Insert
- Delete

The Transaction Log Viewer presents the current state of a record together with its historical changes. Historical versions can be expanded for review, deleted records remain represented in the history, and changed cells are visually identified for Edit actions.

Audit entries include supporting metadata such as:

- Source application
- Loaded application View
- Action performed
- Computer name
- Username
- Windows process ID
- Quality Window version
- Application file and version information
- Override User Name

When a user is logged into Quality Window, the Quality Window username is captured. If no Quality Window user is logged in, the Windows username is captured.

The Transaction Log Viewer is context-sensitive and respects the current Logsheet filter. Records hidden by the active filter are also hidden from the audit viewer. Detailed audit-trail behavior is documented in the [Quality Window Transaction Audit Trail - User Guide](#).

Administrative Change Audit Trail

Quality Window maintains a separate audit history for changes made to application configuration in QW Admin. This is distinct from the Transaction Audit Trail, which records changes to application data, and the Security Audit Log, which records security and authentication activity.

The administrative change audit trail provides traceability for changes to the structure and configuration of a Quality Window application. Recorded changes can include items such as:

- Variable additions, changes, movement, and deletion
- Specification and limit changes
- Control rule changes
- Other changes to the application definition and configuration

The change history allows administrators and quality personnel to review how an application configuration has evolved over time and provides supporting evidence when investigating or assessing changes to a controlled application.

This capability can support an organization's configuration management, change-control, validation, and data-integrity processes by maintaining a history of changes that may affect how application data is collected, evaluated, or presented.

Application Change Archives

In addition to recording administrative changes, Quality Window automatically creates a complete archive of the application whenever an update is made in QW Admin. These archived copies provide a historical record of the application configuration associated with administrative changes and can support change review, troubleshooting, validation, and recovery activities.

Security Audit Logging

In addition to application-data transaction history, Quality Window provides a Security Audit Log for security-related activity recorded by Security Administrator.

Security audit categories include user changes and authentication activity. Recorded events can include:

- User creation, updates, and removal

Quality Window in Regulated Environments - Product Controls

- Password changes
- Permission changes
- Successful and failed login attempts
- Authentication method used
- Application accessed
- Machine used during authentication

Depending on the event category, audit records can include date and time, user information, authentication method, application, machine name, success or failure status, failure reason, and source application.

The Security Audit Log Viewer supports filtering, grouping, sorting, pagination, and export to CSV or Excel to assist with review and investigation.

Backup and Recovery

QW Admin includes utilities for backing up and restoring Quality Window applications. Access to the Tools and Utilities area that contains these functions can be restricted through Quality Window administrative permissions.

Quality Window also automatically creates a full archive of the application when updates are made in QW Admin, providing an additional recovery point for application configuration changes.

Because Quality Window is deployed within the customer environment, the organization remains responsible for defining and operating its overall backup, retention, restore, disaster-recovery, and business-continuity processes.

Software Validation and Change Assessment

Busitech provides build-specific [Quality Window validation documentation](#) that customers can use as supporting evidence within their own software-validation activities.

Busitech also maintains [QW release notes](#) describing enhancements, new functionality, resolved issues, and build-specific changes. Together, validation documentation and release notes can support an organization's assessment of software updates and change-control requirements.

The organization using Quality Window determines the validation scope appropriate to its intended use, risk assessment, quality system, and applicable regulatory requirements.

System Requirements

Quality Window uses the published [Quality Window system and installation requirements](#).

Busitech does not define separate product system requirements solely because Quality Window is being used in a pharmaceutical or other regulated environment.

Organizations may impose additional infrastructure, security, qualification, or operational requirements based on their own policies and regulated use.

Use in Regulated Environments

The controls described in this document can support organizations implementing Quality Window in environments where requirements related to data integrity, user access control, audit trails, controlled data modification, accountability, system security, software validation, change control, backup, and recovery are relevant.

Where regulations such as [FDA 21 CFR Part 11](#) are applicable to a customer's use of Quality Window, these QW capabilities may form part of the technical controls used by the organization. The applicability of a regulation and the adequacy of the complete implementation depend on the customer's intended use, configuration, infrastructure, procedures, personnel controls, validation activities, and quality system.

Supporting Quality Window Documentation

The following Busitech documentation provides additional detail for the capabilities summarized in this document:

- [Quality Window Security - Admin Guide](#)
- [Quality Window Transaction Audit Trail - User Guide](#)
- [Quality Window 6 Release Notes](#)
- [Build-specific Quality Window validation documentation](#)
- [Quality Window system and installation requirements](#)
- [Quality Window application backup and restore guidance](#)

Customers should use the documentation applicable to the QW build they are evaluating or operating, particularly when performing validation or formal change assessment.