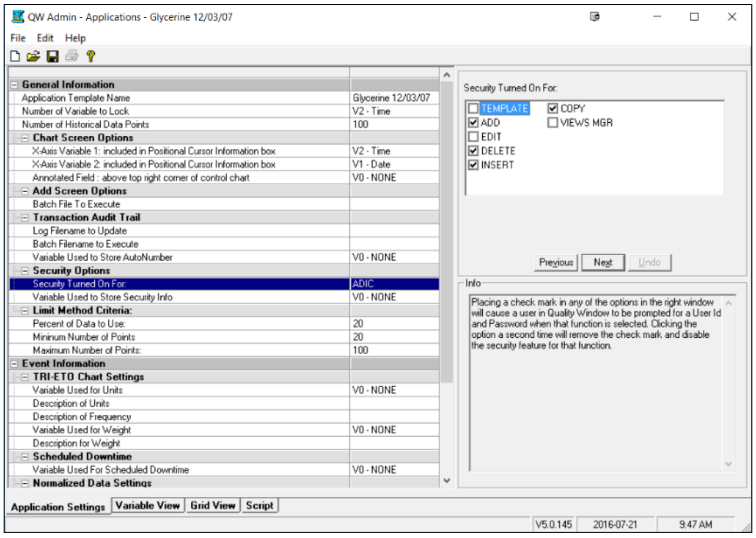
Enhanced Security in QW 5 (build 801+)

An enhancement has been made to the way security is handled in Quality Window 5. Previous to this build, every QW application can have one or more flags set depending on what functionality they want restricted. Here is a screenshot of what that looks like:



What this means is, if any user opens this QW application and tries to perform one of the functions checked off, then QW will prompt the user for a valid Userid and Password. If the userid/password matches in the security database, then the action is granted. One of the problems with this is, if a user is defined in the security database, they basically can perform all actions that are checked, and if they're not in the database, they cannot perform any actions. It's basically all or nothing, and there was no way to define users as particular roles.

In this new version, each user can now have a set of rights defined to them. The way this is done is by placing 'rights' into the existing User Identification property of the security database as follows:

Created : Oct 5, 2016

By placing individual rights, enclosed in square brackets, you are stating that this user, when prompted for an action, assuming they enter their proper password, will be allowed to perform that particular action. In the example above, User1 and User2 would only be allowed to 'T' open an application, or 'A' add a new record. User Validator, would be allowed to 'T' open an application and also 'V' open Views Manager. A special right called '*' means that the user can perform all actions, as in Ray and Supervisor. If you specify [], you are saying that this user can perform no rights. Admin was set to this to give a user access to managing the security database, but no access to any applications. The possible rights available are as follows:

T	Open an application template
A	Add a new record
E	Edit an existing record
D	Delete an existing record
I	Insert a record
C	Copy a record
V	Open the Views Manager
*	All of the above rights

Caution: If no square brackets are found for a user, they actually have full rights since the system will default to the way it used to work. Also, if you do not set an action for an application, then it doesn't matter what rights you give to a user, they will be able to perform that action. For example, if you don't check Delete for an application, and a user tries to delete, it makes no difference if that user has Delete rights or not, they will have access – in fact, the system will not even prompt for a valid Userid and Password.

If you do choose to use this functionality, another change you will see is that if you have defined a **Field to Store Security Information** in an application, then instead of how it used to return the User Identification value, if it finds square brackets, it will instead return the User Name value into that application's field.

Also note that in build 801+, the location of the security database is determined by the properties set in the utility program called QW5SharedConfig.exe which can be found in the Windows Start Menu, or in the Busitech\QW50\ folder.