Protection of knowledge and knowledge bases

Knowledge system protection

Quaestor has several ways to protect and encrypt knowledge based systems. This protection can be divided into:

1. General protection
2. Knowledge protection:
    a. Knowledge based system user level protection
    b. Parameter value protection
    c. User specific encryption
3. Solution protection:
    a. Project file protection

Click here to download an Excel sheet presenting a matrix of possibilities and limitations for the different user levels.

1 General protection

Without any specific action, user rights of any knowledge based system is based on your user type/level. In short: an End-User and Domain Expert are only able to open (protected or unprotected) projects and will never be able to open a knowledge base. Furthermore, an End-User cannot see detailed information about relations (knowledge). A Knowledge Engineer can do anything with a protected or unprotected knowledge base and project (if the appropriate password is available).

After saving and reopening, every knowledge base is by default protected against removing frames. You always have to remove protection (either the password protection or the default protection) by selecting Unprotect file in the File menu.

Please note that a user of the demo/reader version of Quaestor (which can be downloaded for free...) is Knowledge Engineer and thus can see knowledge and modify a knowledge base in unprotected knowledge bases with the only limitation that this knowledge base should be smaller than 100 frames. Thus with a reader version any knowledge base smaller than 100 frames without any specific password protection can be modified and all its relations etc. can be seen. When a reader version opens a knowledge base larger than 100 frames, all knowledge can be viewed and modified but this knowledge base cannot be saved. Realise this when sharing important/proprietary knowledge bases...

2 Knowledge protection

2.1 Knowledge based system user level protection

To limit the user type/level for a specific knowledge base, a Knowledge Engineer can protect the knowledge base with a password. This enables the downgrade of user type/level for users (and Knowledge Engineers working in a project).

As mentioned, this functionality is only available as Knowledge Engineer and can be found in the Quaestor menu under File>Protect file.

2.2 Parameter value protection

In addition to protection of your knowledge base, you can protect a specific value in a knowledge base. For instance a value that enables an advanced mode you do not want to share with all users.

In that case you can password protect the change of this specific parameter value.

You have to be Knowledge Engineer to password protect values.

When you want to password protect values, first of all you have to give the relevant parameter a fixed knowledge base value (see Properties). Hereafter, select the parameter and choose in the right mouse menu "Protect Input...". You will get a dialog to give your password.

Note that you cannot see the password anymore after you have provided it and closed the dialog.

If you have the appropriate rights to modify the knowledge base (which you have if you are able to protect a value...), you are able to undo the password protection of values. Select the relevant parameter and select in the right mouse menu "Unprotect Input".

To modify the password you have to undo the previous protection and repeat the above action.

2.3 User specific encryption

When you want to make sure that (in addition to the protection above...) only specific users can start the knowledge base, you can encrypt the knowledge base file itself. When protected, only users with the correct decryption key are able to open the knowledge base.

This protection can be combined with the protections above.

When you want to use this functionality, you have to be Knowledge Engineer.

Moreover, Qnowledge is able to provide Quaestor with a license string including built-in encryption. This means that knowledge bases saved with a Quaestor version with this license string can only be used by Quaestor versions using the same license string. On request this technology can be used for your specific application.

WARNING: Qnowledge cannot help or decrypt knowledge bases if you lose your encryption key! So safeguard this key very carefully.

3 Solution protection

3.1 Project file protection

Every project can be protected in two ways:

1. protection against unauthorized opening
2. protection against unauthorized modification

In this way you can make sure that either users can only open a project when they have the correct password (but when the have the password they can do everything based on their own user type/level) or can only open modify the project when they have a password but are always able to open the project read-only.

In case a project is protected against unauthorized modification, an End-User will automatically open the project read-only.

When you want to use this functionality, you have to be at least Domain Expert.