Datgel DATA SOLUTIONS
Geotechnics • Geoenvironment • Laboratory

User Guide

Datgel
Security Tool gINT Add-In

DST-UG-001 - 1.5
May 2009

Disclaimer

The information in this publication is subject to change without notice and does not represent a commitment on the part of Datgel Pty Ltd. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software must be used or copied only in accordance with the terms of the agreement.

Every effort was made to ensure accuracy of this information. However, Datgel Pty Ltd makes no warranty as to the correctness of this information or the supplied files.

Datgel Pty Ltd
Suite 8, Level 1, The Hub
89 - 97 Jones Street
Ultimo NSW 2007
Australia

Tel: +61 2 8202 8600
Fax: +61 2 8202 8606

Email: info@datgel.com
Website: www.datgel.com

Contents

Tables

About Datgel Security Tool

The Datgel Security Tool gINT Add-In allows for greater control over editing and deletion of data, restricts access to gINT commands and hides application groups from users. It allows the database administrator to build a customisable user interface for gINT based on the needs of particular users. The security is based on a user group defined for each user and domain or computer combination. The security definition is made in gINT library tables.

Note: Editing of the library tables are generally restricted to the database administrator to prevent conflicts and increase project security and integrity.

You need to complete the installation procedure (see Installation and Licensing on *page 1*) and activate (see *Datgel Product Licensing System User Guide*) before you can use the Security Tool.

Support

12 months support and maintenance is included with the license purchase. For technical support please email support@datgel.com or call +61 2 8202 8600.

System Requirements

gINT

The product runs optimally using gINT 8.2.003 or higher, however it will run using gINT 8.1 or higher.

The product will run using gINT Logs, gINT Logs Plus, and gINT Professional.

Hardware and Operating System

Same system requirements as gINT 8.2, see: http://www.gintsoftware.com/products_requirements.html.

Required Windows Components

1. Windows Installer 3.1
2. .NET 3.5 Framework SP1

Conventions and typography used in this guide

Note: Tips and additional Information to help you.

>	Used to indicate a series of menu commands. e.g. Select **File > Open**.
|	Used to indicate a gINT Application Group, Application, Table Group or Table , e.g. **DATA DESIGN | Project Database**
Bold Text	Items you must select, command buttons, or items in a list. e.g. Navigate to **UTILITIES | Convert Projects** (4th tab).
Italics Emphasis	Use to emphasize the importance of a point such as parameters. e.g. Data Entry – Check *Omit Must Save prompt when save is required*
CAPITALS	Names of keys on the keyboard. for example, SHIFT, CTRL, or ALT.

KEY+KEY	Key combinations, for example CTRL+P, or ALT+F4.
`Code Snippet`	Indicates a code snippet within a paragraph
`Code sample`	Indicates a sample program codes inserted in user guide e.g. `public override string ToString ()`
`File name or path`	Used for formatting file name and paths e.g. `di_lib.glb` or `V:\10 gINT\Datgel Install Files\`
Table_Name	Database table name, e.g. POINT_TABLE.
Field_Name	Database field name; e.g. PointID
Command line	Command line, presented exactly as it must be entered e.g. **cdir**

1 Installation and Licensing

1.1 Installation Overview

There are four parts to the installation process:

- Install DLL program
- Merge gINT library objects
- Merge gINT project table to your project file and your data template
- Activate the product license

The *first three* steps can be performed in any order and are described below. The activation procedure must be done last and is described in the *Datgel Product Licensing System User Guide*.

1.2 Package Contents

Your software purchase may have come with the following contents:

- Applications CD which normally has the following folders:
  `\gINT Files`
  `\Datgel Network License Server`
  `\Documentation`
  `\Installation files`
- A hardware license key

1.3 Before Installation

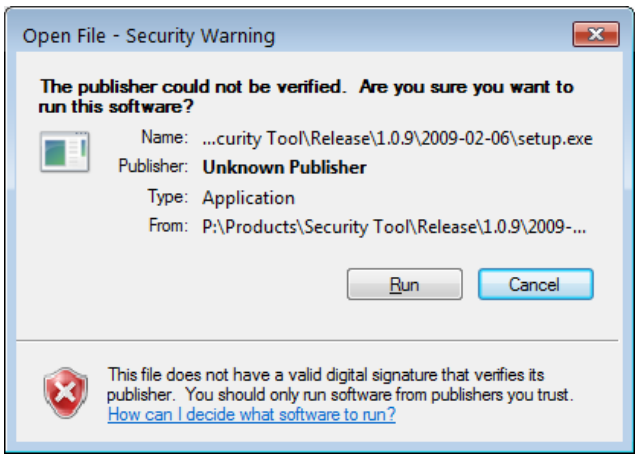
A few basic preparations can help ensure an effortless installation.

- Make sure that the computer where you plan to install the program meets the minimum hardware and software requirements.
- Connect your PC to Internet before installation (must have a working Internet connection).

  The Security Tool requires that the Microsoft .NET 3.5 framework SP1 is installed on the PC prior to the installation of the Tool. If your PC does not have the .NET 3.5 framework SP1 installed, then it will be automatically downloaded and installed during the Tool installation process.
- Log into the PC with Administrator privileges before starting installation.
- It is recommended that you exit out of other applications that maybe running on your PC.
- Close gINT before you start installation.
- Keep the serial number and license number handy.

1.4 Install DLL Programs

1. If you received an installation CD, then insert the CD and browse to the folder `\Installation Files`
2. Double click the file named `Setup.exe`
3. Click **Run** to begin installation.



Follow the on screen instructions when installation begins:

4. Click **Next** on the *Welcome to the Datgel Security Tool Setup* dialog.

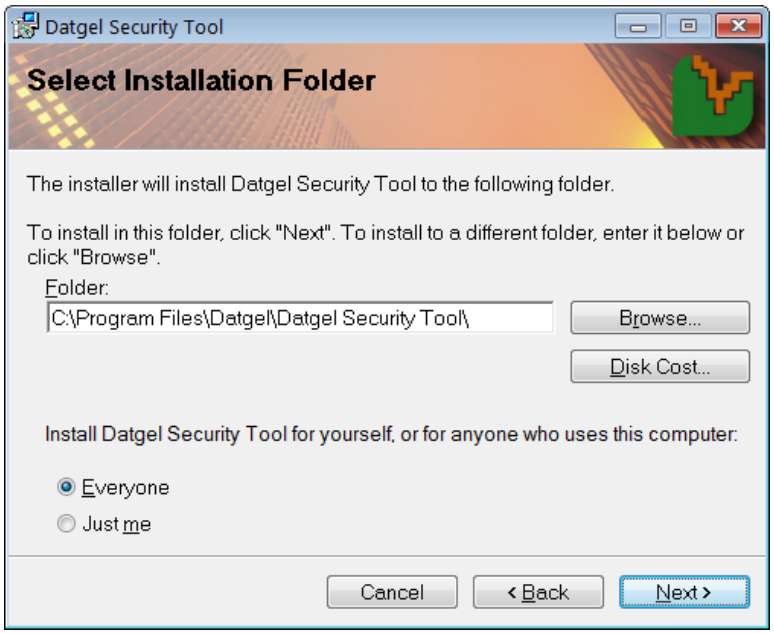
5. Scroll and carefully read the *License Agreement*, and choose option **I Agree**, and click **Next.**

Alternatively choose *I Do Not Agree* and click Cancel if you disagree with the license agreement. The installation will stop and exit.

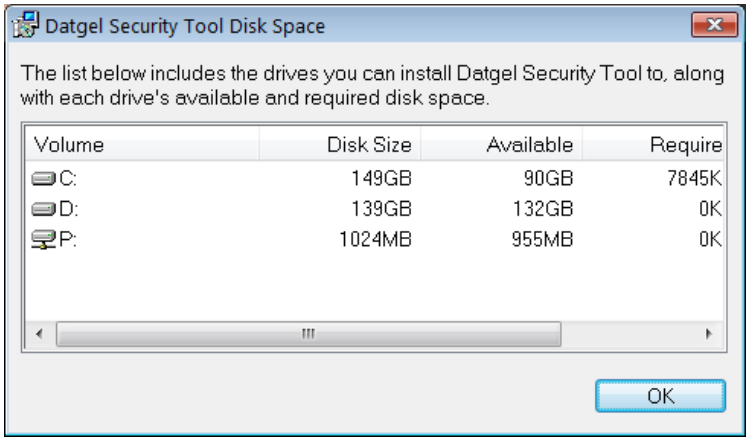
6. On the *Select Installation Folder* dialog, either accept the default folder (recommended) or select **Browse** to specify the folder where you want to install the Security Tool Add-In.

   Leave *Everyone* bulleted to indicate that anyone logged onto the PC can use the Security Tool Add-In.

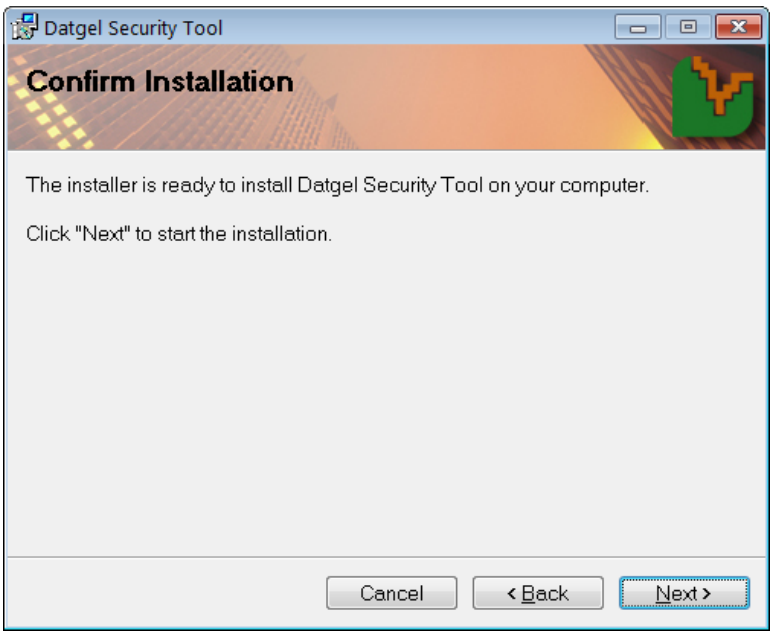
   Click **Next** when ready.



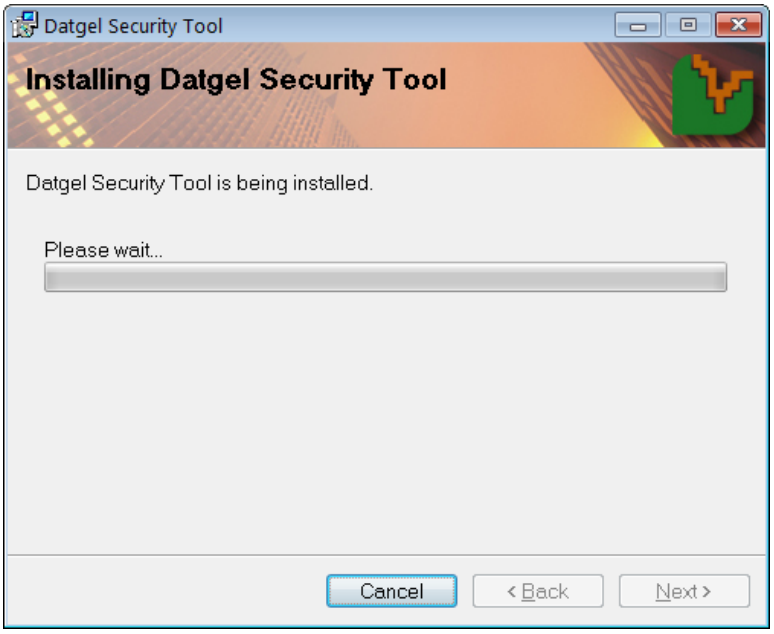
OPTIONAL Click on **Disk Cost** to view the disk space statistics. Click **OK** when done.



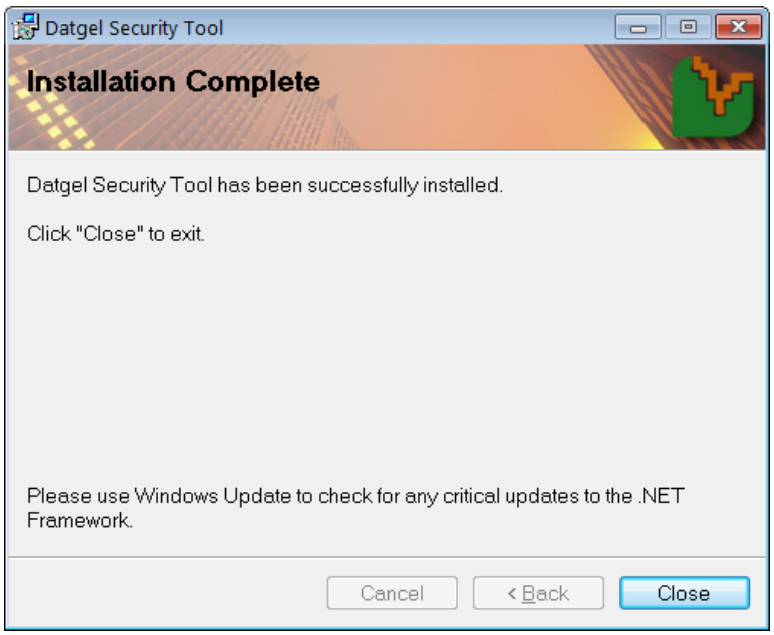
7. Click **Next** to start installation.



8. Observe the progress bar to monitor installation progress



9. Click **Close** when the *Installation Complete* dialog is displayed.



1.5 Merge gINT Library Objects

IMPORTANT In the trial version of the Security Tool gINT Add-In, the library will be locked and you cannot merge any gINT Library Objects into your Library file, or make changes to this Library file. In this case, you have to use the locked library as-is.

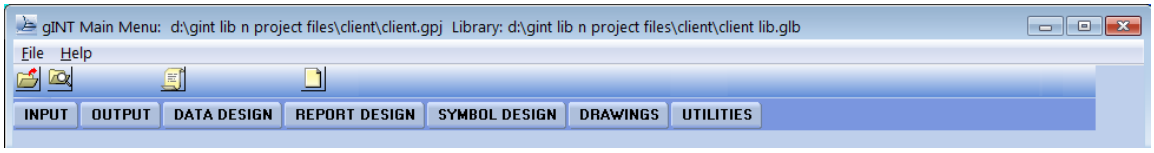
If you have purchased the Security Tool gINT Add-In, then you have full access to the library objects, and you may proceed with the following steps to merge the gINT Library components into your Library file.

1. Make a backup copy of your existing library file. By default this is located at:

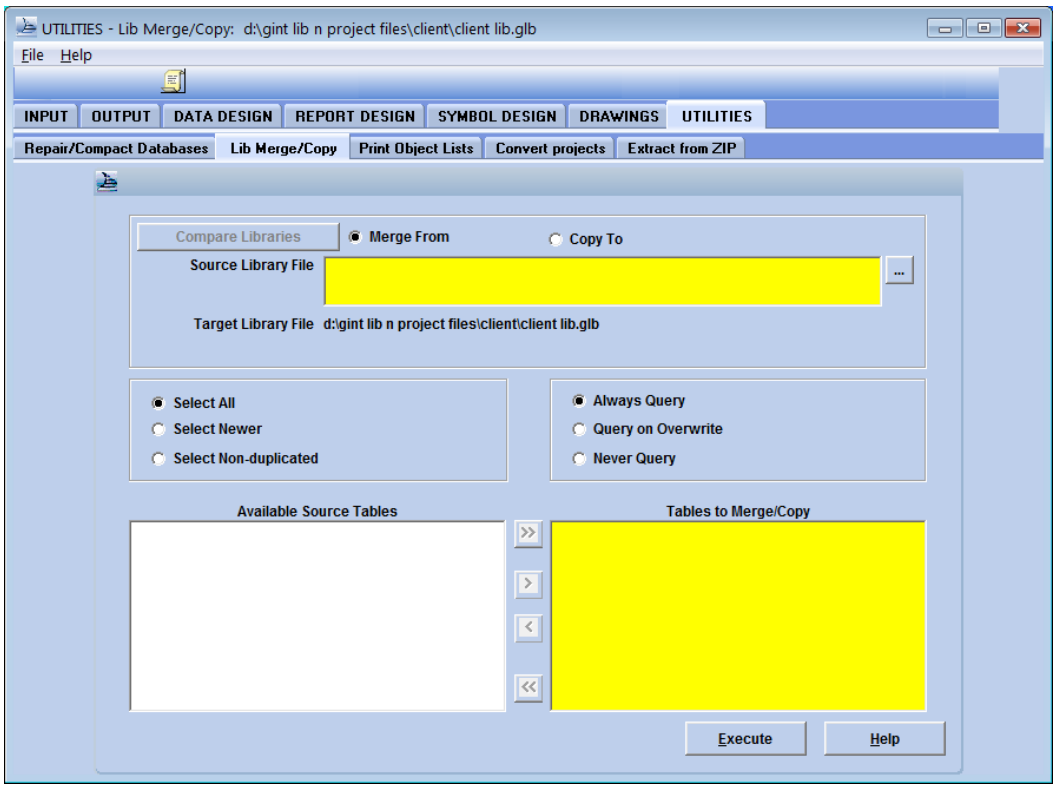
   `C:\Program Files\gINT\libraries\`

2. Start gINT and open the library and project file you wish to use with Datgel Security Tool gINT Add-In.

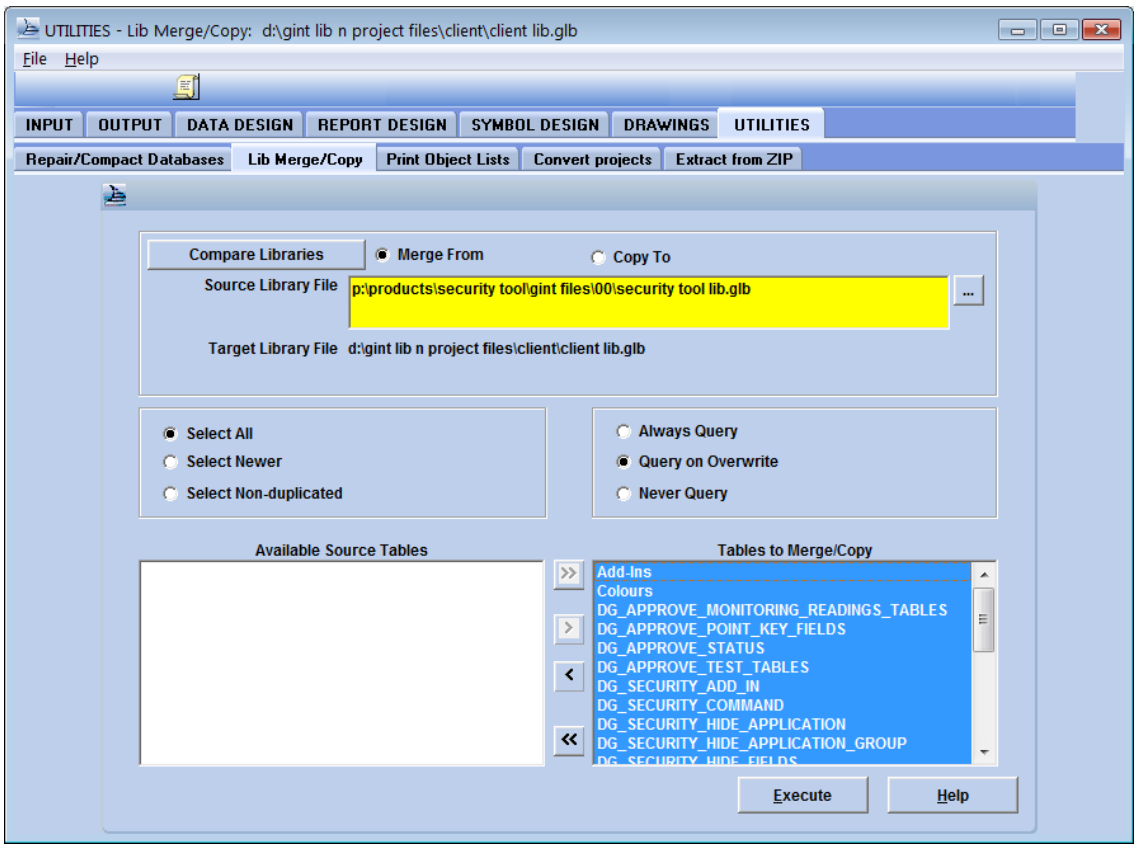
   The opened project and library files are displayed at the top of the gINT Window.



3. Select **UTILITIES > Lib Merge/Copy**.

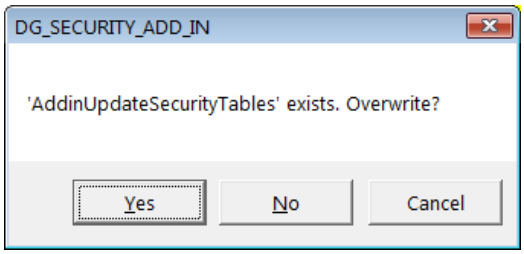


4. Check the bullet that reads **Merge from**.
5. In the *Source Library File* pane, browse the installation CD for file `Datgel Security Tool## lib.glb` where `##` is the version number.
6. Check the bullet that reads **Select All**.
7. Check the bullet that reads **Query On Overwrite.**
8. Click  button to move all tables from the *Available Source Tables* pane on the left to the *Tables to Merge/Copy* pane on the right side.



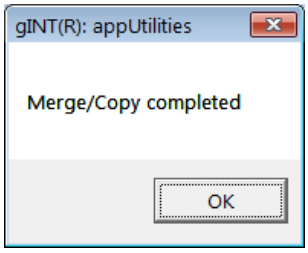
9. Click **Execute**.

   Take care to read the overwrite dialog and click **Yes** if you wish to overwrite the file, ELSE click No.



   This will merge in the security tables listed in the introduction, the Add-In menu item, and gINT Rules modules which are all related to the Tool.

10. Click **OK** to finish the merge.



1.6 Merge gINT Project Tables and Fields

1. Make a backup copy of your existing project file. By default this is located at:

   `C:\Program Files\gINT\projects\`

2. Start gINT and open the library and project file you wish to use with Datgel Security Tool.

3. Select **DATA DESIGN > Project Database**.

4. Select **File > Open File > Current Project…** to open your current project file.
5. Select **PROJECT Table** from the yellow drop down list.
6. Select **Tables > Merge Fields from Other Files...** then browse the installation CD and select the file `Security Tool ##.gpj`

   Click **Open.**
7. Browse and select a table.
8. Click **Open to see** a list of available tables.

9. Select **PROJECT** and click **OK**.
10. Click **Mark All** and click **OK**.
11. Click **Save**.

This will merge the fields required for the linked database function and the hide by project scenario type function to the Project table.

Other tables and fields in `Security Tool ##.gpj` are provided as examples, and don't need to be merged into your project file.

1.7 Activate License

After installation (and before using the Security Tool Add-in), activate the user license as described in Chapter 3 of the *Datgel Product Licensing System User Guide*.

Note: You only need to activate this product when you run the Datgel Security Tool in gINT 8 for the first time.

1.8 Secure Library

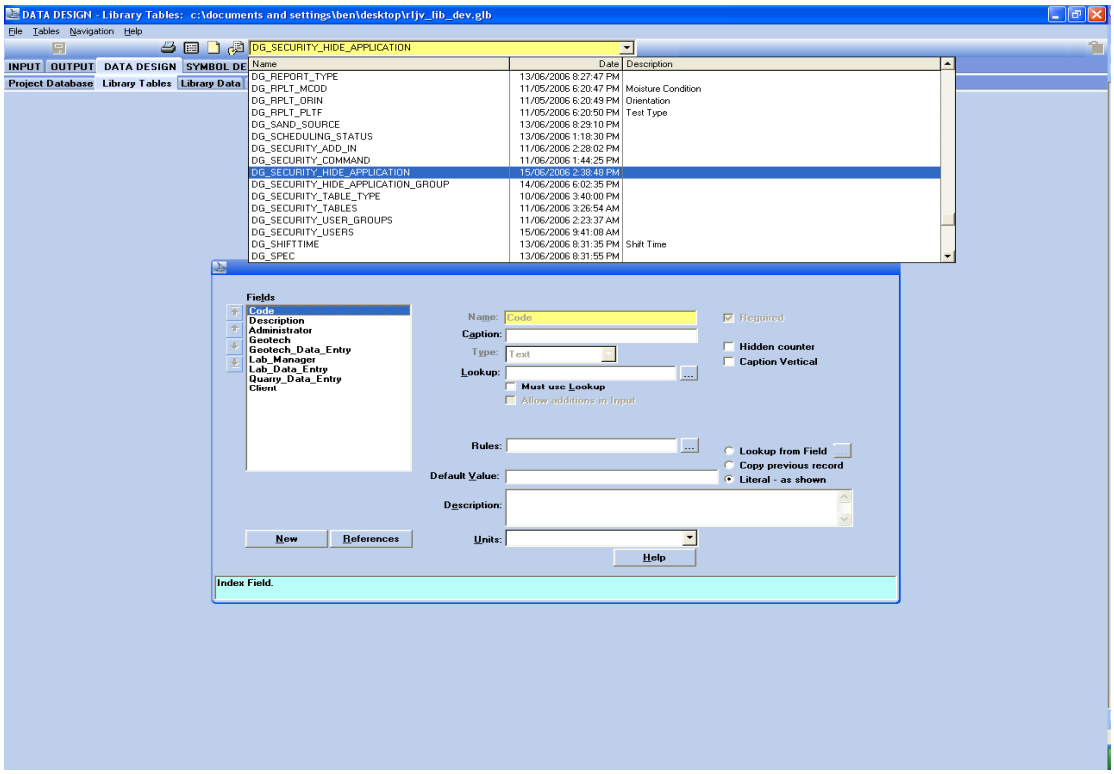
The library must be secured in order to stop non-administrative users from configuring the user rights. Refer to the gINT Online help page *Secure Library (Command)*.

2 User Rights and Interface by Group and Status

This section discuses how to control the Editing and deletion of project data based on Status and/or User Group, and the options to hide gINT applications and application group (tabs) based on User Group.

2.1 Library Tables

1. Select **DATA DESIGN | Library Tables**, and then select the appropriate security table from the yellow drop down list.



The relevant tables are:

- DG_SECURITY_ADD_IN
- DG_SECURITY_COMMAND
- DG_SECURITY_HIDE_APPLICATION
- DG_SECURITY_HIDE_APPLICATION_GROUP
- DG_SECURITY_PROJECT_TABLES
- DG_SECURITY_STATUS
- DG_SECURITY_TABLE_TYPE
- DG_SECURITY_TABLES
- DG_SECURITY_USER_GROUPS
- DG_SECURITY_USERS

The purpose and usage of these tables are explained in further detail throughout this user guide.

Note: Editing of these tables is generally restricted to the database administrator to prevent conflicts and to increase project security and integrity.

2.2 Adding a New User - DG_SECURITY_USERS

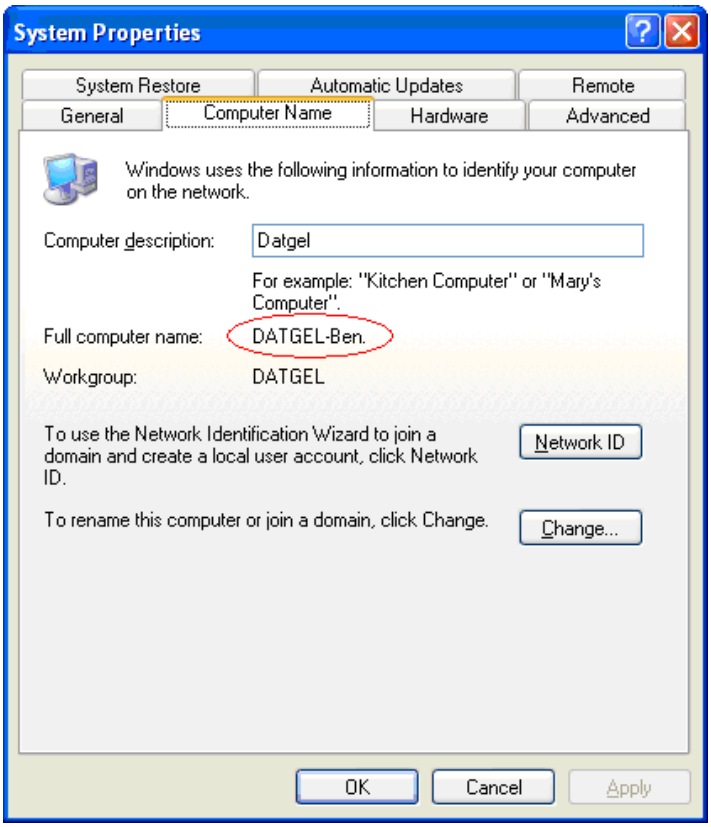
To enter a new user you need the user's Domain or *Computer Name*, and *User Account Name*. The Domain takes precedence over the Computer Name, and you don't need both.

2.2.1 Step 1: Gather Domain, Computer Name & User Account Name

Note that the domain may be displayed as e.g. *datgel* or *datgel.local*. You may store the domain name in either syntax.

2.2.1.1 In Windows XP environment

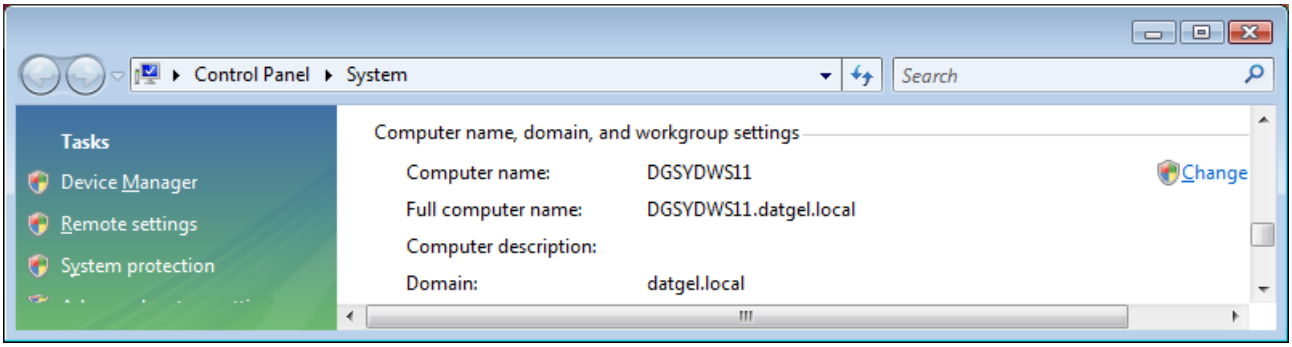
1. Select **Start > Control Panel > System**.
2. Click the **Computer Name** Tab to view the *Computer Name* and *Domain*.



3. Select **Start > Control Panel > User Accounts** to view the *User Account Name*.

2.2.1.2 In Windows Vista environment

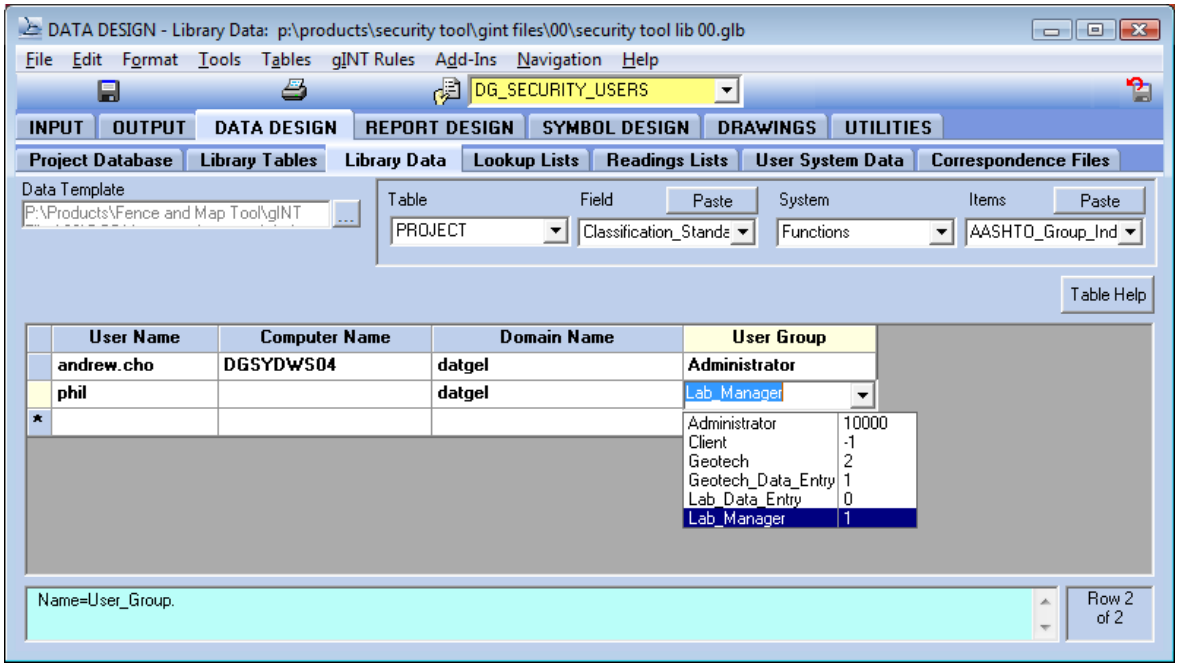
1. Select **Start > Control Panel > System** and scroll to view the *Computer Name* and *Domain*.



2. Select **Start > Control Panel > User Accounts** to view the *User Account Name*.

2.2.2 Step 2: add a new user

1. Start gINT and open the library and project file you wish to use with Datgel Security Tool.
2. Select **DATA DESIGN | Library Data**.
3. From the yellow drop down list at the top, select the table DG_SECURITY_USERS
4. Enter the *User Name* and *Domain or Computer Name* and select the *User Group* which you want to apply to this user from the drop down list.

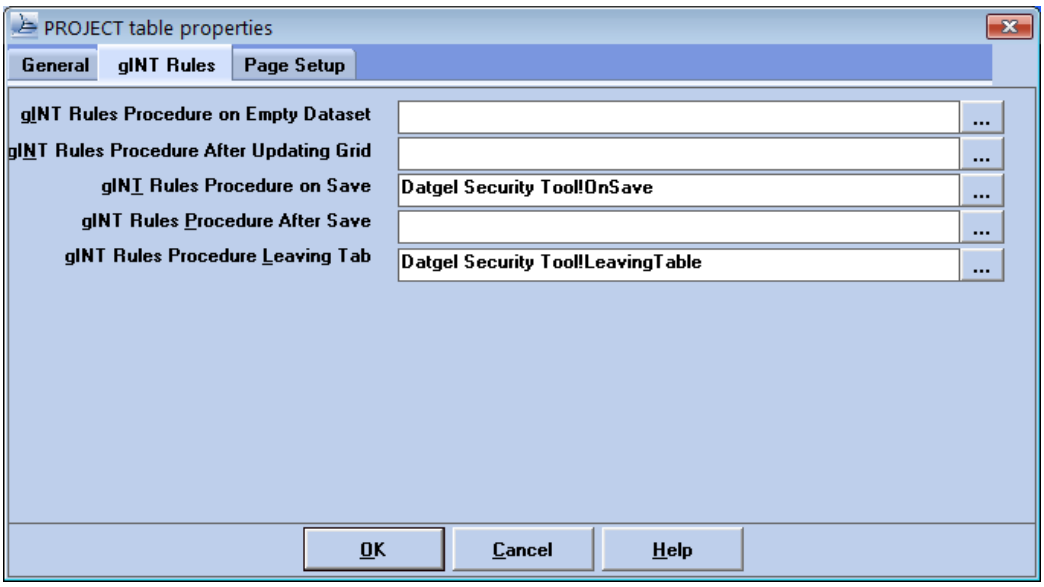


Note: The *User Name, Domain* and *Computer Name* are not case sensitive.

2.3 Assigning gINT Rules Properties

Assigning the gINT Rules properties is crucial for the Security Tool to function properly. Administrators will need to set the properties of every project table they wish to secure.

1. Start gINT and open the library and project file you wish to use with Datgel Security Tool.
2. Select **INPUT | Main Group.**
3. Open a table in the **INPUT** tab (e.g. **Project**).
4. Dispaly the table properties form by selecting  , **Tables > Properties** or pressing **F8**.
5. Click **gINT Rules** tab on the *PROJECT Table Properties* dialog.
6. Enter data beside the rules as shown on the screen bellow:



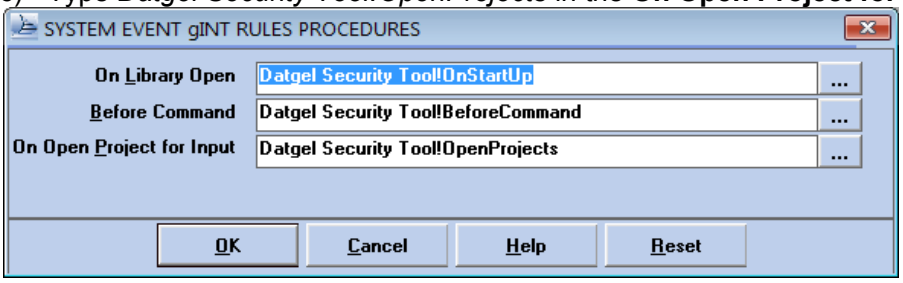
Note: The values for the various gINT Rules are as per the table bellow.

Table 1 Values for gINT Rules

gINT Rules	Value
gINT Rules Procedure on Save	Datgel Security Tool!OnSave
gINT Rules Procedure on Deletion	Datgel Security Tool!OnDelete
gINT Rules Procedure Leaving Tab	Datgel Security Tool!LeavingTable

7. Click **OK**.
8. Repeat steps 3 to 7 for all tables in the database.
9. Select the **INPUT** tab,
10. From top menu, select **gINT Rules > System Events**
11. In the SYSTEM EVENT gINT RULES PROCEDURES dialog

    a) Type *Datgel Security Tool!OnStartUp* in the **On Library Open** field,
    b) Type *Datgel Security Tool!BeforeCommand* in the **Before Command** field.
    c) Type *Datgel Security Tool!OpenProjects* in the **On Open Project for Input** field.



12. Click **OK**.

2.4 Defining User Groups - DG_SECURITY_USER_GROUPS

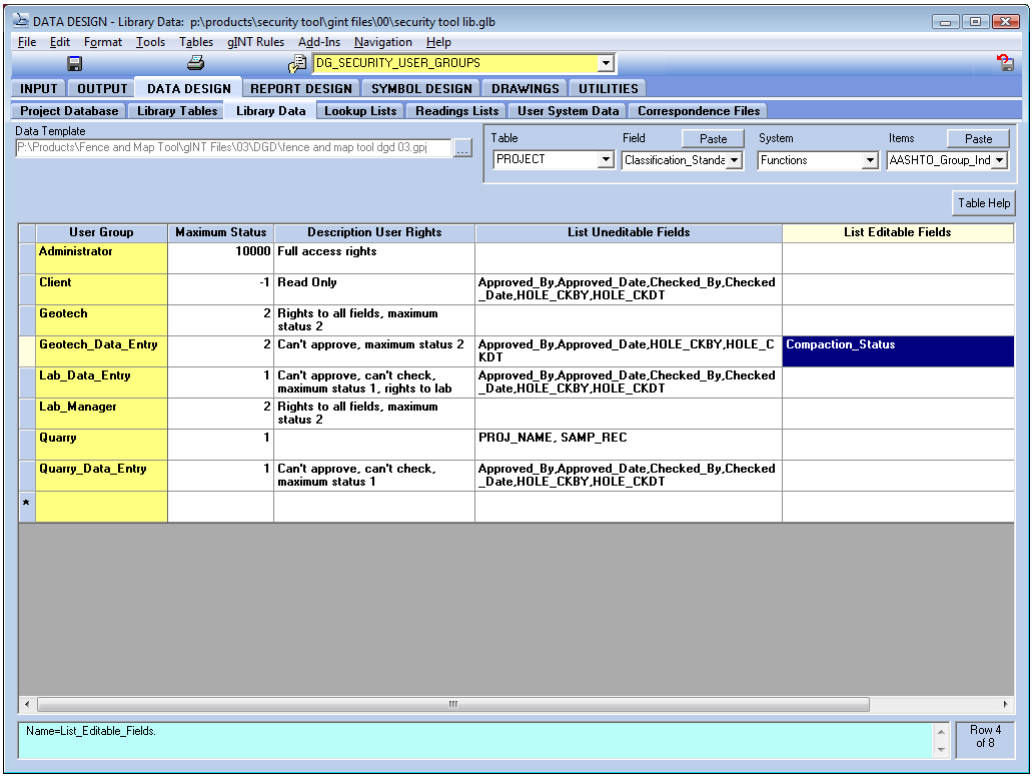
Each user on the system is assigned to a *User Group*. This *User Group* determines their access rights to different commands and applications within gINT. For example, if you were in the group *Administrator* you would generally have complete access to gINT. If you were in the group *Lab Data*

Entry you might not be able to export and import data, generate reports or change library data such as that in the security tables. User Groups are defined in the library table DG_SECURITY_USER_GROUPS.

To define a User Group, you need to

- give it a name,
- assign it a maximum status, and
- Optionally provide a List_Uneditable_Fields, List_Editable_Fields, and Description.

When defining a new User Group, you should never use spaces in the name; always use underscores to separate the words, for example **Lab_Data_Entry**.



2.4.1 Maximum Status

For every new User Group you must provide it with a Maximum_Status. This is an integer assigned to that particular User Group that dictates the highest status of the data processing that a user may edit data. For example, Proposed = -1, Preliminary = 0, Final Release to Client = 3. When entering data in **INPUT** tab, for every unique PointID there is a status for that record which defines the stage in data processing a user is at. Generally, keep the status between -1 and 100 where the maximum status allocated to a user (administrator) is 10,000.

2.4.2 Description User Rights

This is a place to describe the User Group's rights in layman's terms and has no direct influence on any calculations.

2.4.3 List Uneditable Fields

When adding a new User Group, we may provide a list of fields that we do not want the group to have access to. This list must be provided in comma or carriage return separated form with no spaces and with the field names exactly as they appear in the tables. Great care should be taken to include underscores and not to ignore capitalisation and not to use any quotation marks or brackets.

For example:

Approved_By,Approved_Date,Checked_By,Checked_Date,HOLE_CKBY,HOLE_CKDT is correct.

Approved_By ,Approved_Date, Checked_By, Checked_Date, HOLE_CKBY, HOLE_CKDT is incorrect.

“Approved_By”,”Approved_Date”,“Checked_By”,“Checked_Date”, “HOLE_CKBY”,“HOLE_CKDT” is incorrect.

2.4.4 List Editable Fields

For each User Group we may define a comma or carriage return separated list of fields that the User Group can always edit. The required syntax is the same as for List_Uneditable_Fields, however the meaning is the opposite.

Example usage: Say we have set the Point_Status on the POINT table to 3, which restricts all non Administrator users from editing that PointID, however we want to allow some non-Administrator User Groups to set the Compaction_Status field. By entering **Compaction_Status** in List_Uneditable_Fields for a given User Group you will enable that user Group to always change Compaction_Status, regardless of the Status of the PointID.

2.4.5 Adding New User Groups to Other Tables

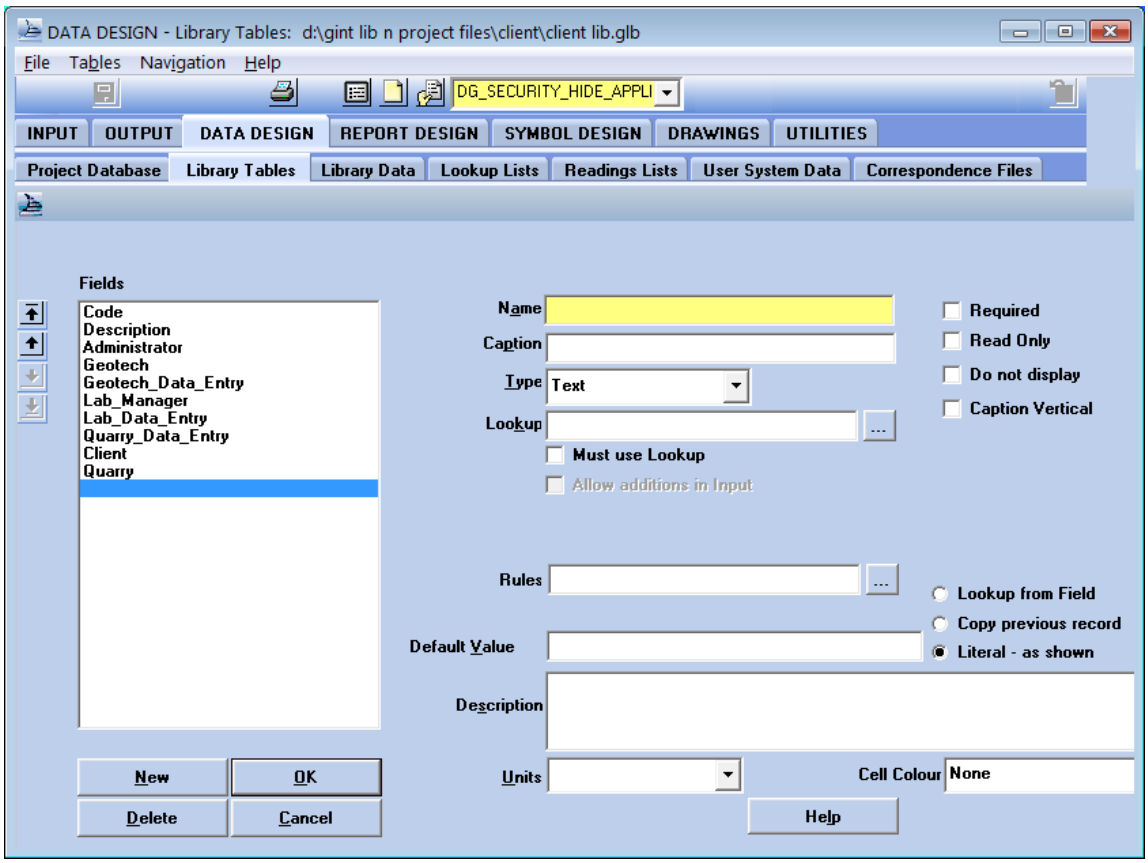
When you add a new User Group in the table DG_SECURITY_USER_GROUPS, it is vital that you also add the field to the following tables:

- DG_SECURITY_ADD_IN
- DG_SECURITY_COMMAND
- DG_SECURITY_HIDE_APPLICATION
- DG_SECURITY_HIDE_APPLICATION_GROUP
- DG_SECURITY_TABLES

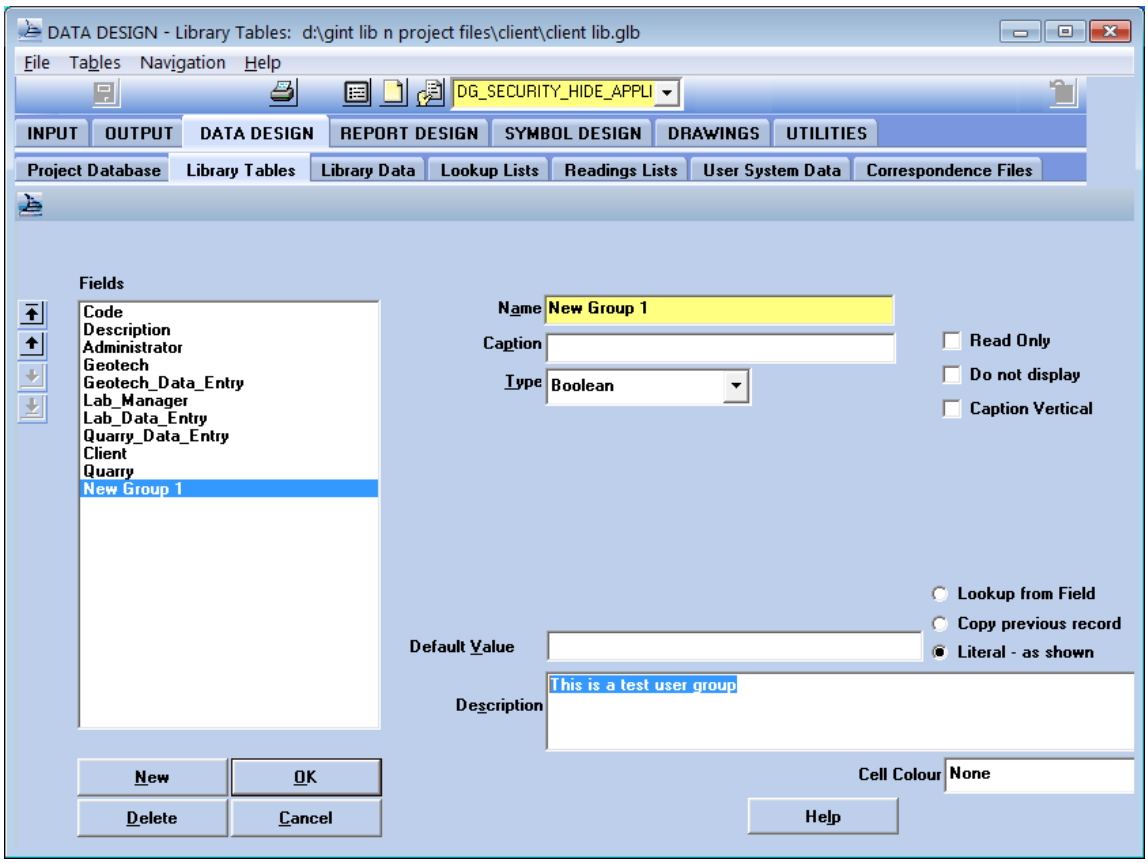
Without adding these fields you will not be able to customise the appropriate security features.

To add the fields, you must replicate the following procedure for all the above tables.

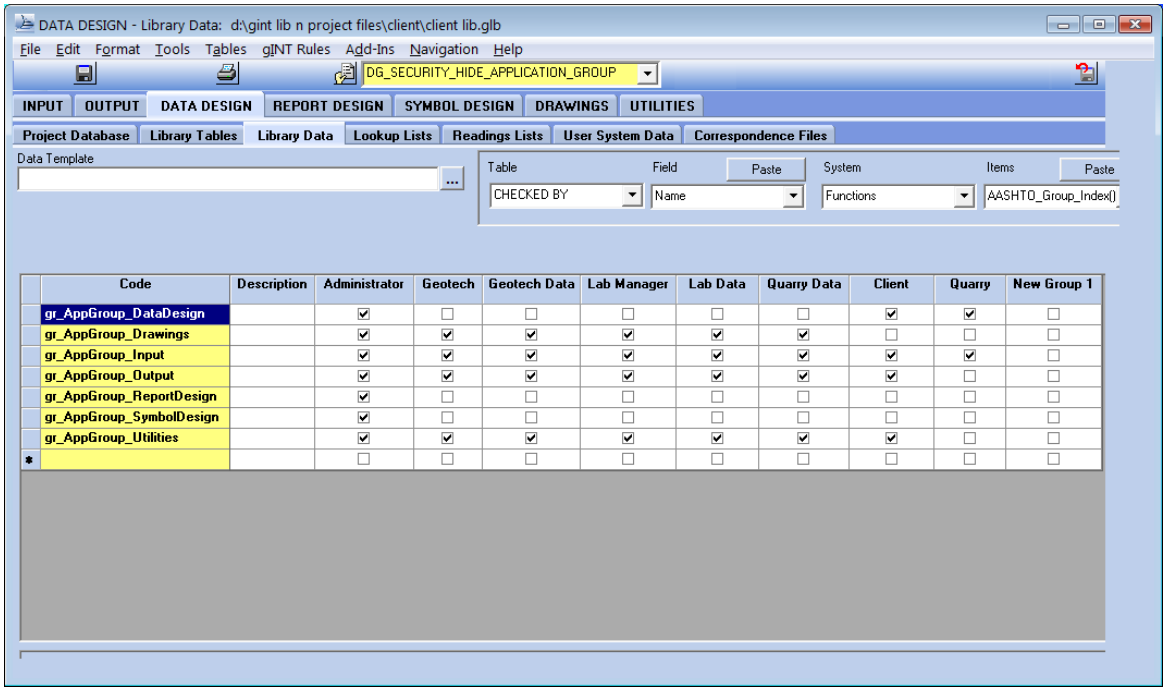
1. Select **DATA DESIGN | Library Tables**
2. From the yellow drop down list, select the table DG_SECURITY_HIDE_APPLICATION_GROUP



3. Click on the **New** button under *Fields*
4. In the *Name* field, type in the new User Group name
5. Under *Type*, select **Boolean**
6. Under Description, you may enter a description of the user group (optional)



7. Click **OK** when finished.
8. Click **Library Data** tab for the same table to see the new field as below.



2.5 Defining Tables - DG_SECURITY_TABLES

For every new project table created in gINT, it must be defined in the security system. This is done in the library table DG_SECURITY_TABLES as follows:

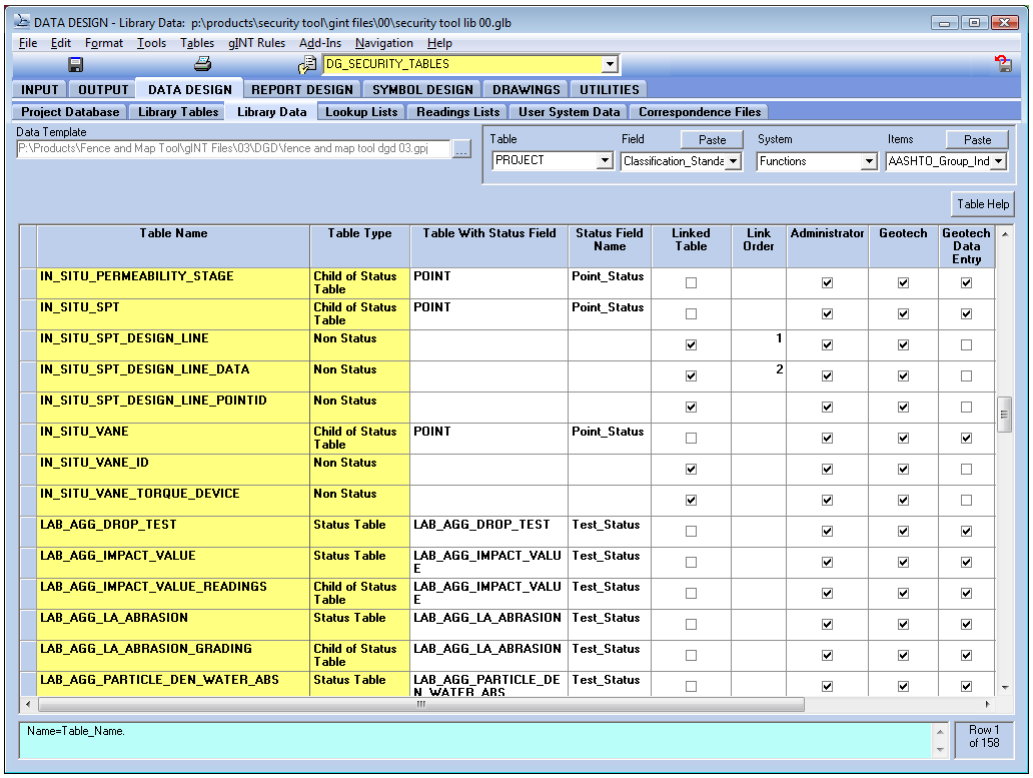
1. Click **INPUT** tab and open an appropriate project file.

2. Select **Add-Ins > Datgel Security Tool > Update Security Tables**

Note : For all tables not listed in DG_SECURITY_TABLES you will be asked if it should be added.

Do not add the gINT system tables.

3. Once complete, then go to DG_SECURITY_TABLES and add the rest of the required data.
4. Select **DATA DESIGN | Library Data**, and select DG_SECURITY_TABLES from the yellow drop down list to view the table.



2.5.1 Adding a New Table to the Security System

Under Table Name enter the name of the gINT project table. The table name may not contain spaces but may have underscores.

2.5.2 Table Type

Table type is the relationship of the table you have created to the table that contains the applicable status field e.g. HOLE_STAT. The permissible *Table Type* are:

- Status Table
- Child of Status Table
- One to One of Child Of Status
- Parent of Status
- Non Status

2.5.2.1 Status Table

An example of a *Status Table* would be POINT which has the field HOLE_STAT' or 'RELD which has the field TEST_STAT. If the status field is contained within the table, as above, then you should set the *Table Type* property as **Status Table**.

2.5.2.2 Child of Status Table

A table whose parent table contains the status field would be assigned *Child of Status' under* Table Type. An example of this would be the SAMP table, whose parent table POINT contains the field HOLE_STAT which is the status field for the SAMP table.

2.5.2.3 One to One of Child of Status

This is a *Table Type* which has a one-to-one relationship with its parent table with the applicable status field. An example would be the table DPRG whose parent table POINT contains the status field HOLE_STAT.

2.5.2.4 Parent of Status

This is a *Table Type* whose child tables contain the applicable status field. An example of this might be the CLSS table which is the parent of all lab test tables with TEST_STAT status fields. We wish to stop the CLSS record from being edited or deleted if one of the lab test son a child table has a status in excess of the user's rights.

2.5.2.5 Non Status

This is a *Table Type* which does not have a *Status Field*. An example of this may be FILE.

2.5.3 Table with Status Field

This field needs the name of the gINT table that contains the status field. For example, if the Table_Type is *Child of Status* then the Table_With_Status_Field would be its parent table. In the case of SAMP this would be POINT. If the Table_Type is *Non Status* then you should leave the field blank.

2.5.4 Status Field Name

This is the name of the field that contains the status field. An example would be HOLE_STAT from the POINT table. Note this field is taken from the table defined in the previous entry for Table_With_Status_Field. If it is a *Non Status* table, then we should leave the entry blank.

2.6 Defining Access Rights for User Groups

You can define access rights for User Groups in three tables:

- DG_SECURITY_TABLES
- DG_SECURITY_ADD_IN
- DG_SECURITY_COMMAND

The data in all these tables can be changed (if you are authorised) by going to **DATA DESIGN | Library Data** and selecting the appropriate table from the drop down list.

2.6.1 DG_SECURITY_TABLES

This table allows you to set which tables a particular user group has editing and deletion rights to where the staus is less than or equal to the user group maximum status. If the check box for a particular group is ticked then the user HAS access to that particular table. If it is left unchecked they DO NOT.

2.6.2 DG_SECURITY_ADD_IN

This defines which Add-In commands (found in INPUT and selecting the 'Add-Ins' option) the user is authorised to use. If the checkbox is ticked it means they DO have access.

2.6.3 DG_SECURITY_COMMAND

This defines which commands a user is authorised to use. If the checkbox is ticked the User Group is authorised to use it. Secuity checks are only made on the listed commands. A complete list of gINT commads can be viewed in gINT's Online help page *Summary Table of Commands.*

2.7 Customising the Interface by User Groups

You can control the visibility of gINT Application Groups and Applications based on User Group. This is defined in the following library tables:

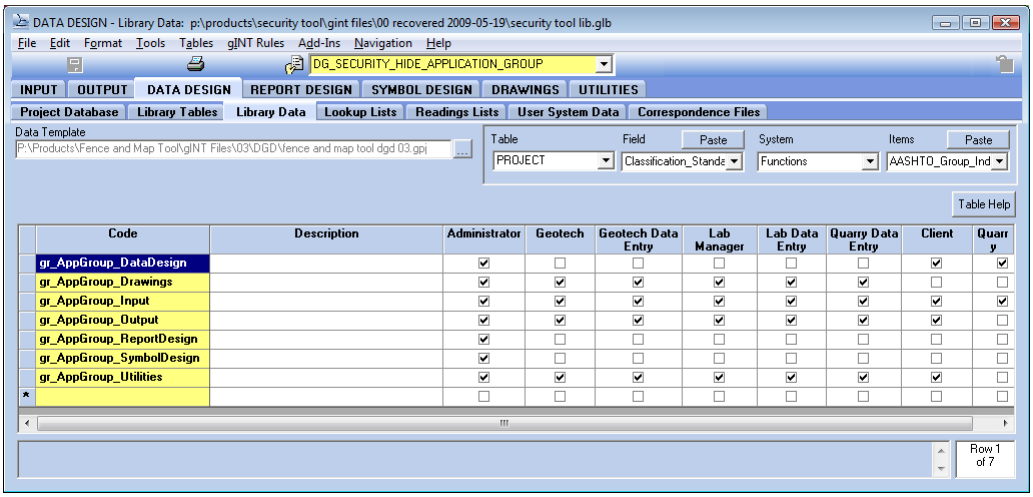
- DG_SECURITY_HIDE_APPLICATION_GROUP
- DG_SECURITY_HIDE_APPLICATION

The data in all these tables can be changed (if you are authorised) by going to **DATA DESIGN | Library Data** and selecting the appropriate table from the drop down list.

2.7.1 DG_SECURITY_HIDE_APPLICATION_GROUP

This customises the interface so that you can hide certain application groups from particular User Groups. If an Application Group is checked it will be shown, otherwise if it is unchecked it will NOT be shown.

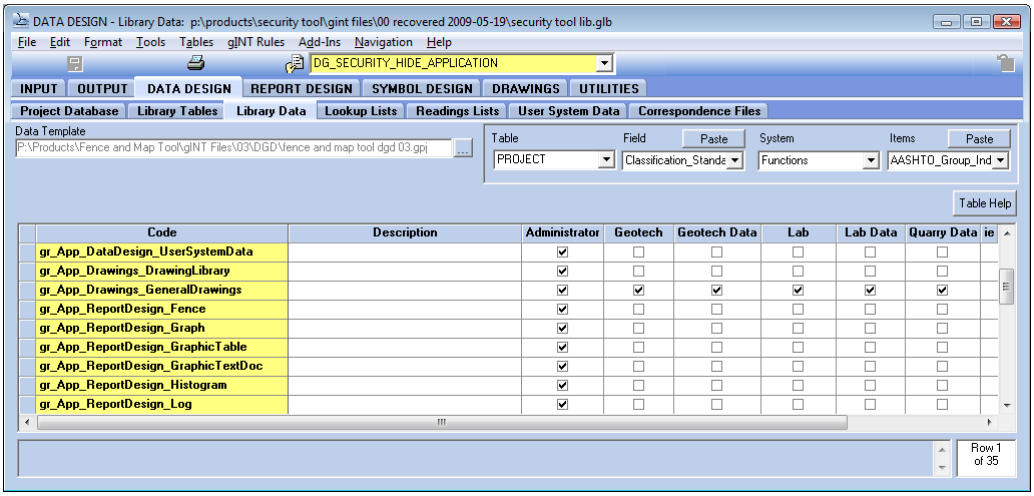
For example if you only wanted to show the **INPUT** and **DATA DESIGN** tabs the only check those boxes for the User Group.



Note : The changes you make to this table will only take effect when you restart gINT.

2.7.2 DG_SECURITY_HIDE_APPLICATION

This customises the Applications you are authorised to see in a given application group. If the group is checked it will be shown, otherwise it WILL NOT appear. For example if you wanted to prevent library data being changed you would have the record *gr_App_DataDesign_LibraryData* as unchecked for whichever user groups you wanted to hide this from.



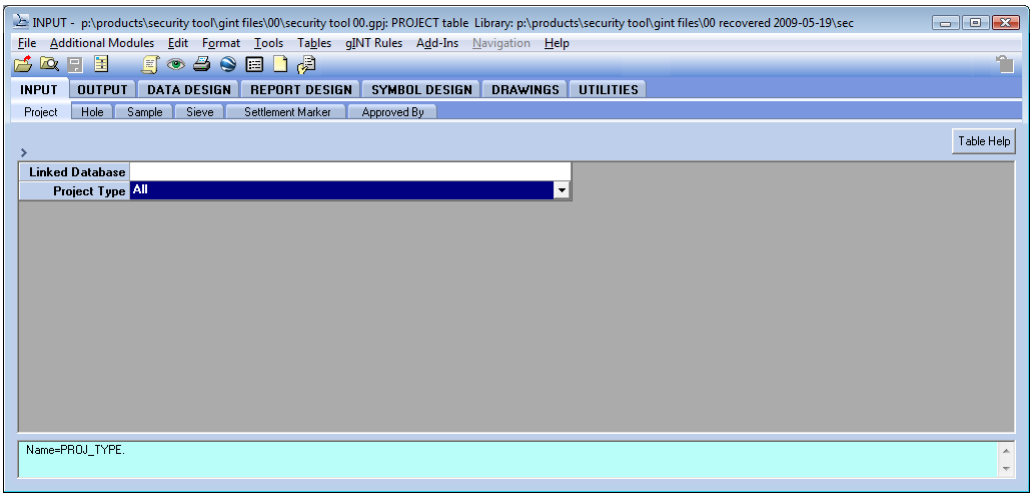
Note: Any changes you make to this table will only take effect when you restart gINT.

3 Customising the Interface by Senario

A user may wish to only display certain tables depending on what they are working on, and hide other irrelevant tables. The scenario type can be changed bt selecting **INPUT | Project** Project_Type field. You can customise the gINT user interface in three tables:

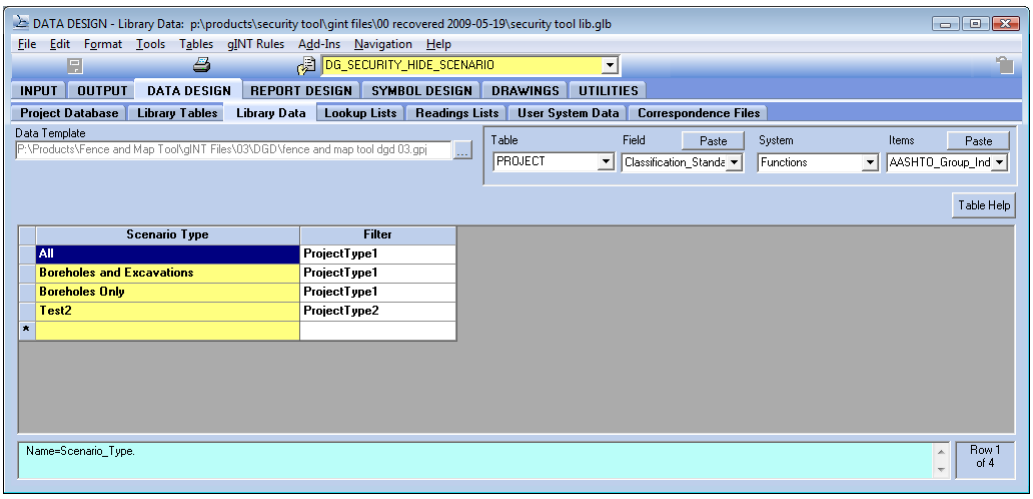
- DG_SECURITY_HIDE_GROUPS
- DG_SECURITY_HIDE_SCENARIO
- DG_SECURITY_HIDE_TABLES

The data in all these tables can be changed (if you are authorised) by going to **DATA DESIGN | Library Data** and selecting the appropriate table from the drop down list.



3.1.1 DG_SECURITY_HIDE_SCENARIO

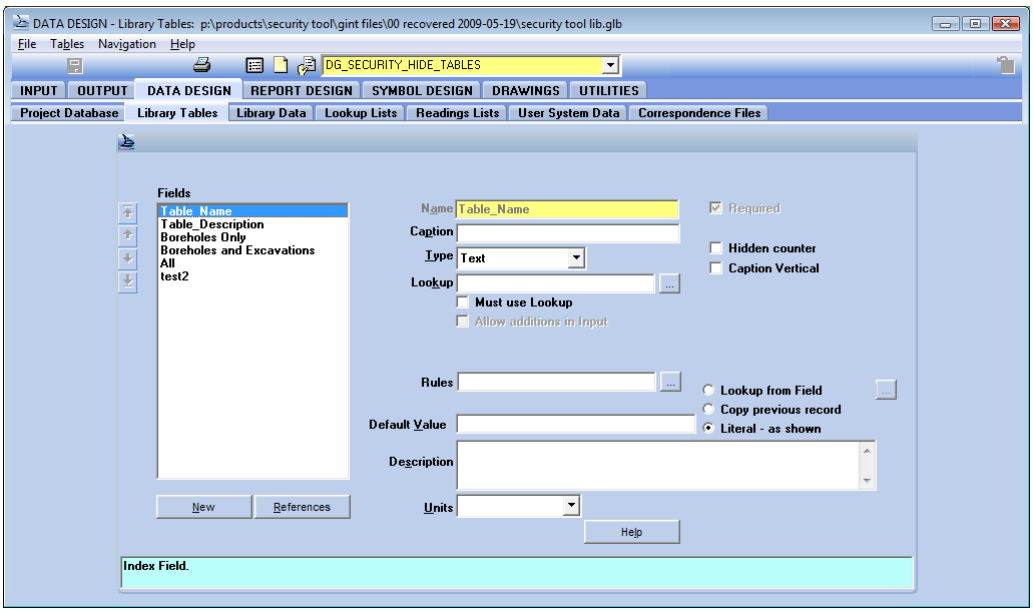
In this table, you may enter the types of scenarios to hide or display the tables by.



When a new Scenario Type has been entered, a new field named after the scenario type must be created in DG_SECURITY_HIDE_TABLES and DG_SECURITY_HIDE_GROUPS.

To do this:

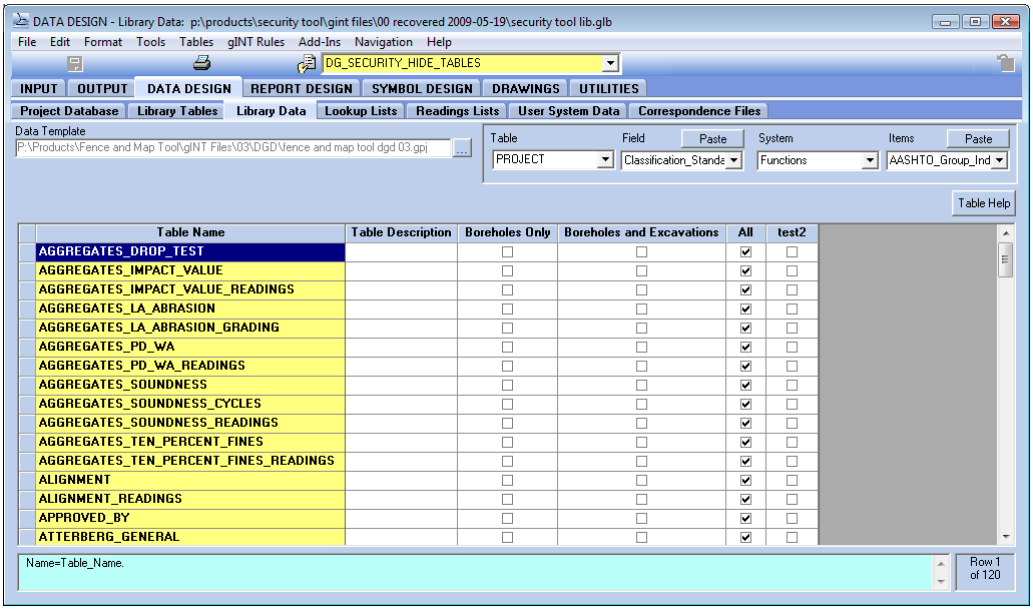
1. Select **DATA DESIGN | Library Tables**, and select DG_SECURITY_HIDE_TABLES.



2. Click on **New**, enter the name as entered in the DG_SECURITY_HIDE_SCENARIO table, and select type as *Boolean*.
3. Click **OK**
4. Repeat this step for DG_SECURITY_HIDE_GROUPS

3.1.2 DG_SECURITY_HIDE_TABLES

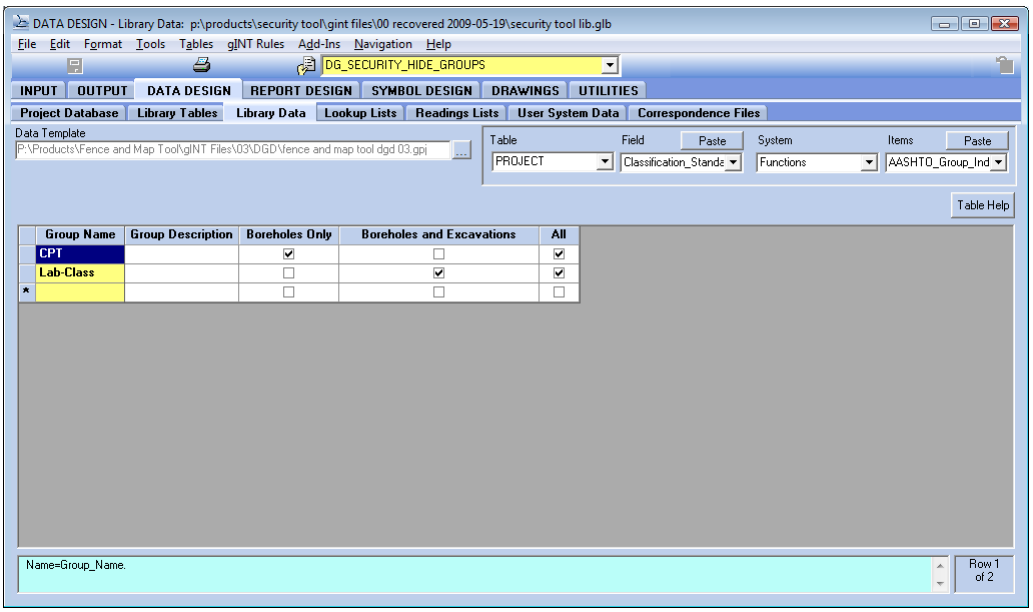
This library table customises the tables to be hidden or displayed depending on the selected scenario type.



Firstly, you must enter the names of the tables you wish to hide on the yellow column. The Check boxes indicate whether or not you want the table to be hidden when the project type is selected. When unchecked, the table will be hidden from view.

3.1.3 DG_SECURITY_HIDE_GROUPS

This table customises the table groups to be hidden or displayed depending on the selected scenario type.



Firstly, you must enter the names of the table groups you wish to hide on the yellow column. The Check boxes indicate whether or not you want the table group to be hidden when the project type is selected. When unchecked, the table group will be hidden from view.

4 Linked Database

This option applies where multiple gINT project files exist, and most require all the same lists and sitemaps. The database concept makes easier to maintain the same list and map data in all databases.

Example: Create a new *Calibration* gINT project file. Make sure it has all the list and calibration data you require, and the newest sitemap. Then set the field on the PROJECT table Linked_Database to the *Calibration* database path and file name for each of the working projects. Don't enter anything in the Linked_Database field for the *Calibration* project file.

To update the linked data run the command **Add-Ins > Datgel Security Tool > Update Linked Tables**. Do this in each of the working project files. You will not be allowed to edit the linked tables in the working projects; you must go to the "Calibration" project file to edit the data.

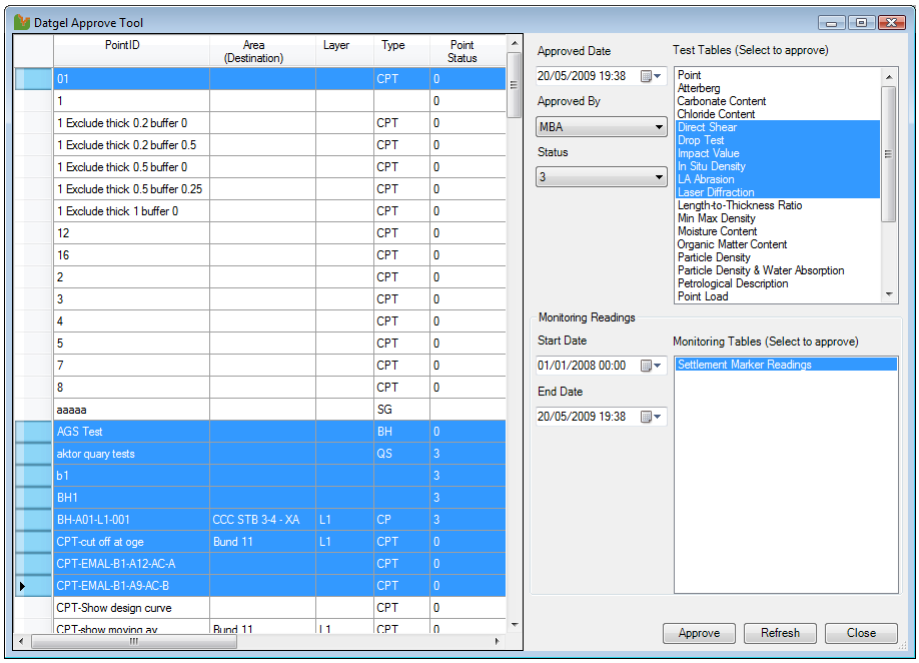
You can see which tables are linked by going to **DATA DESIGN | Library Data** DG_Security_Tables, the Linked_Table check box defines which tables are linked. The Link_Order field defines an order for copying the data across so that parent data is copied before child data.

5 Approve Tool

The Approve Tool sets Approved By and Approved Date fields in Point, Lab and Monitoring tables as defined in Library Tables. The Approve Tool should only accessible and configurable by Administrators and can be opened from **Add-Ins > Datgel Security Tool > Approve Tool**.

5.1 Usage

1. Set the Status, Approved By, and Approved Date as required.
2. Set the Point and lab (depth related) tables you wish to approve by selecting the tables in the test tables list. You can select multiple tables by both clicking and dragging up or down on a table, or by pressing the ctrl button and clicking on an unselected table. You can deselect by pressing the ctrl key down while clicking on a selected table.
3. Set the monitoring tables (date time tables) and reading date range you wish to approve by selecting the tables in the Monitoring Readings table list. You can select multiple tables by either clicking and dragging up or down on a table, or by pressing the ctrl button and clicking on an unselected table. You can deselect by pressing the ctrl key down while clicking on a selected table.
4. Select the PointID rows you wish to approve by selecting the PointIDs in the PointIDs list. You can select multiple PointIDs by either clicking and dragging up or down on a table, or by pressing the ctrl button and clicking on an unselected PointID. You can deselect by pressing the ctrl key down while clicking on a selected PointID.
5. Click Ok to set the approved by and approved date values.



5.2 Update Rules

Existing data in Approved By, Approved Date and Test Status on Test Tables will always be overwritten.

Approved By, Approved Date and Test Status fields for Monitoring readings will be updated if both the following are satisfied:

- The reading date satisfies the start and end date range

and

- The existing status is less than the new status

5.3 Configuration

The displayed fields in the Point table, the test tables list, monitoring readings tables list and the Approved By list can be configured as required. The Point Table fields, Test Tables List and Monitoring Readings tables List configuration settings are stored in Library Tables.

The Approved By list is defined by the values in the project table APPROVED_BY, which is generally located in the Lists group in INPUT.

The Library Tables and fields related to configuring the Approve Tool described in the following sections:

5.3.1 DG_SECURITY_APPROVE_POINT_KEY_FIELDS

1. Field_Name: The name of the field in the POINT table
2. Field_Caption: The display name of the field, the Approve Tool will display the caption if a value is entered, otherwise it will display the field name.
3. Column_Width: Sets the column display width to the specified value.
4. Order_of_Appearance: Use this to set the order the fields appear from left to right.

5.3.2 DG_SECURITY_APPROVE_MONITORING_TABLES

1. Table_Name: The name of the date time related table.
2. Table_Caption: The display name of the field the Approve Tool will display the caption if a value is entered, otherwise it will display the field name.
3. Approved_By_Field_Name: The name of the field which the Approved By value is to be written to.
4. Approved_Date_Field_Name: The name of the field which the Approved Date value is to be written to.
5. Date_Field_Name: The name of the field which contains the date time value which the Approve Tool should look up to determine if the record is in between the start and end dates.
6. Status_Field_Name: The name of the field which the Status value is to be written to.
7. Table_Order_of_Appearance: Use this to set the order of the tables appear from top to bottom. The numbered tables will take precedence, and the remaining unnumbered tables will be listed in alphabetical order.

5.3.3 DG_SECURITY_APPROVE_TEST_TABLES

1. Table_Name: The name of the depth related or point level table.
2. Table_Caption: The display name of the field, the Approve Tool will display the caption if a value is entered, otherwise it will display the field name.
3. Approved_By_Field_Name: The name of the field which the Approved By value is to be written to.
4. Approved_Date_Field_Name: The name of the field which the Approved Date value is to be written to.
5. Status_Field_Name: The name of the field which the Status value is to be written to.
6. Table_Order_of_Appearance: Use this to set the order of the tables appear from top to bottom. The numbered tables will take precedence, and the remaining unnumbered tables will be listed in alphabetical order.

5.3.4 Configuration Validation

The DG_SECURITY_APPROVE_POINT_KEY_FIELDS must contain PointID in the Field_Name. The Approve Tool will not open if the PointID value is not found in the Field_Name field in this table. Non-existent field names in the Field_Name field on this table will cause the Approve Tool to fail to load.

Invalid or Non-existent Table_Name, Approved_By_Field_Name, Approved_Date_Field_Name, Date_Field_Name or Status_Field_Name in DG_SECURITY_APPROVE_MONITORING_TABLES or the DG_SECURITY_APPROVE_TEST_TABLES library tables will cause the Approve Tool to fail to load.