Author	**ALH, BMW, HBE, LJN, WMS**	Create date	**02-Dec-03**
Project	**Section Access in QlikView**	Last save date	**24-Jul-06**
Subject	**Data protection and security in QV**	Classification	**Public**

Data protection and security in QlikView

Content

1. Data protection and security in QlikView

QlikView has taken data retrieval and analysis to a higher level. However, with such an ease of gathering data from disparate sources it is of great importance to provide excellent protection of data.

This document provides information on how data protection and security is handled in QlikView. It also provides some examples of how to apply different security settings when providing BI data to your work force.

1.1. Section Access

In QlikView the security settings of the qvw-file is set in the script. Access rights and User Levels are defined in the *Section Access* part of the script. Section Access can be used to set access restrictions to data, sheets and sheet objects.

All access control is managed via files, SQL databases or inline clauses in the same way as QlikView normally handles data. If an access section is defined in the script it must be followed by the statement Section Application in order to load normal data.

```
Section access;

SQL SELECT
USERID, PASSWORD, ACCESS, GROUP
FROM
USERS;

Section application;
```

1.2. Section Access system fields

Access levels are assigned to users in one or several tables loaded within the S*ection Access*. These tables can contain several different user-specific system fields, typically USERID and PASSWORD, and the field defining the access level, ACCESS. The full set of section access system fields are described below. Other fields like GROUP or ORGANISATION may be added to facilitate the administration, but QlikView does not treat these fields in any special way. None, all, or any combination of the security fields may be loaded in the access section. However, if the ACCESS field is not loaded, all the users will have ADMIN access to the document and the section access will not be meaningful. It is thus not necessary to use USERID – a check can be made on serial number only.

- **ACCESS** A field that defines what access the user should have.
- **USERID** A field that contains a user ID that has the privilege specified in the field ACCESS.
- **PASSWORD** A field that contains an accepted password.

- **SERIAL** A field that contains a number corresponding to the QlikView serial number. Example: 4900 2394 7113 7304

- **NTNAME** A field that contains a string corresponding to a Windows NT Domain user name or group name.

- **NTDOMAINSID** A field that contains a string corresponding to a Windows NT Domain SID. Example: S-1-5-21-125976590-467238106-1092489882

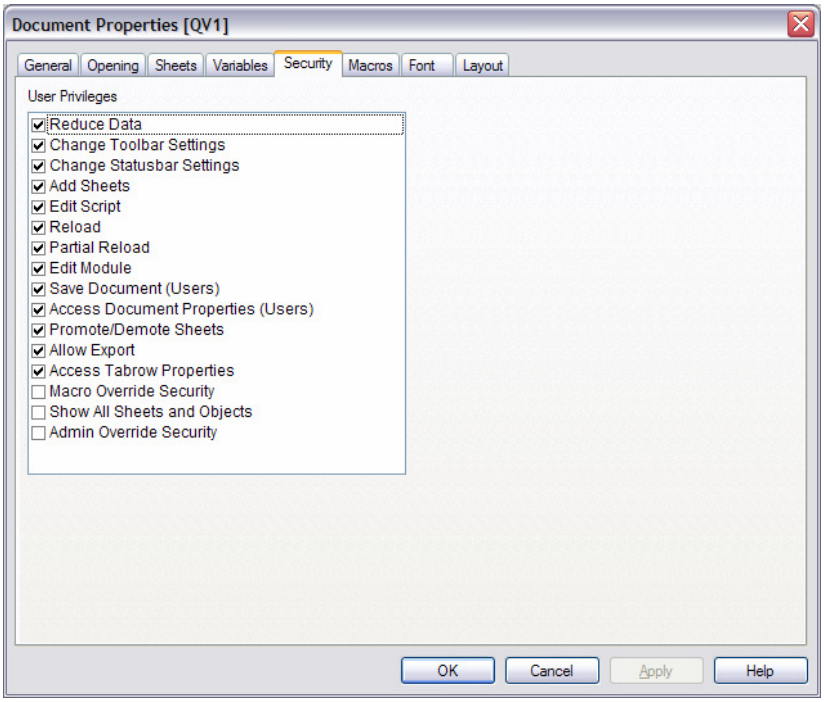
- **NTSID** A field that contains a Windows NT SID. Example: S-1-5-21-125976590-467238106-1092489882-1378

In the QlikView Script, there is a button launching the *Access Restriction Table Wizard* for editing Section Access.

This document gives you some useful examples of how to use the most common configurations in Section Access. For more detailed information about the different fields and how they are used, please *read QlikView Manual Book 1: Installation, Script and Macros,* chapter IV.

1.3. User levels

There are basically three different access levels to a QlikVeiw document. These are ADMIN, USER and NONE. ADMIN gives the person logging in, access to every part of the document including the Security tabs located in *User Preferences, Document* and *Sheet Properties*.



Below you find an example of a basic use of Section Access where different user levels are given to Bob and Bill in accordance with their different userid's and passwords.

```
Section Access;

Load * Inline
[ ACCESS, USERID, PASSWORD
ADMIN, BOB, AAA
USER, BILL, BBB ];

Section Application;
Load… from…
```

Note! UserId and password are ***not*** case sensitive. No matter how you have typed it in the Section Access, it will be changed to upper case by QlikView when a user tries to login.

2. Data reduction on Open Document

In QlikView data can be reduced based on the log in when opening a document. This method was originally developed for QlikView Server, but can also be used in standalone QlikView. It's called "Reduction based on Section Access". An example on where this method could be useful is to prevent a salesperson from having access to other salesperson's information, or to limit employees from seeing information that only should be available to the CEO.

Reduction can be made on loaded data, limiting access for a specific region, cost center, etc. The reduction works by connecting a field and its values in Section Access to a field in Section Application and specifying what value/values the data reduction should be based on. It is also possible to limit access to certain objects in the QlikView document (for example hiding a sheet).

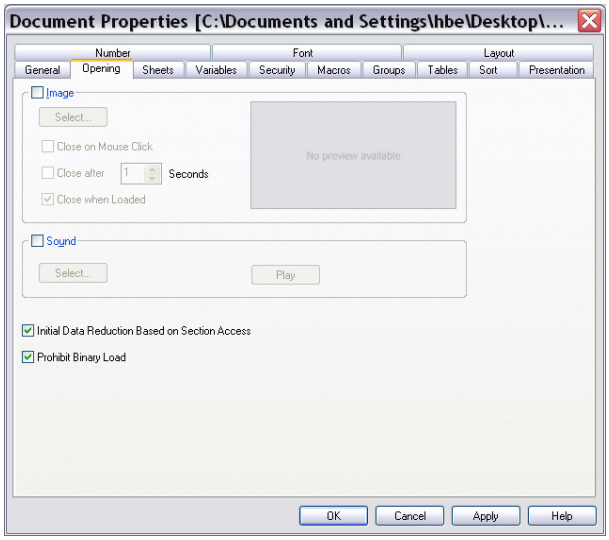
Note! *This field (and the field values) must be in upper case in the section application, since everything in section access will be turned into upper case. To transform the values into upper case you may use the function Upper().*

2.1. Property settings for data reduction

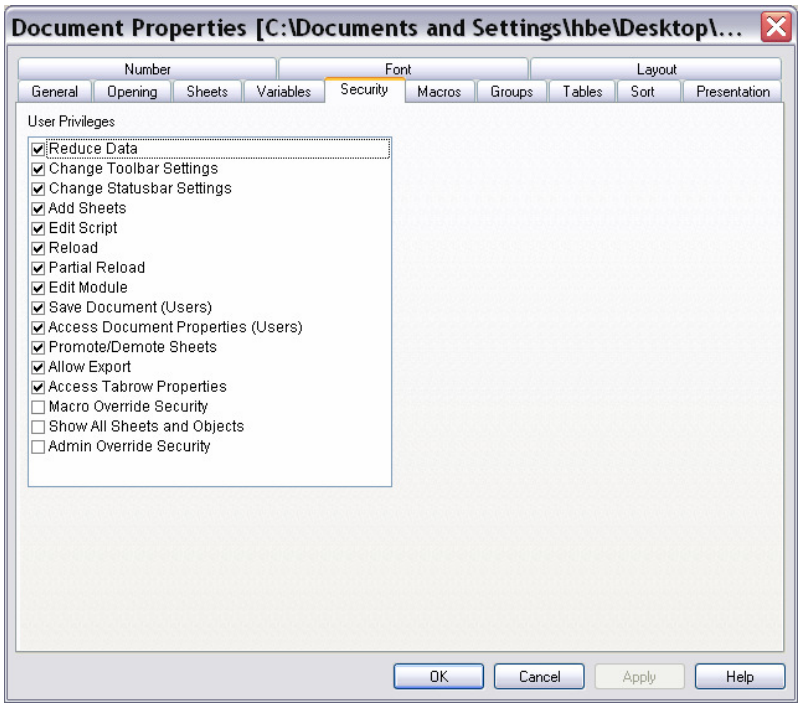
You must also set QlikView to make an initial data reduction by checking the *Initial Data Reduction Based On Section Access* on the Opening page of the Document properties. If you are to use this method in stand alone QlikView, you must also check *Prohibit binary Load* on the same tab.

QlikView 7.01 and newer versions

To prevent discrepancy in the field connecting section access with section application, you should also make sure *Strict Exclusion* is checked on this page. This option is not available in earlier versions.



Note! *A user of an application that is reduced on opening should never be allowed to save the document under the same name (The application would then only hold the reduced values). Also, users should never be allowed to run the script since all data then would be loaded into the application. This can be prevented by checking the appropriate check boxes on the Security tab in Document Properties.*



2.2. Data reduction on certain field values

Data reduction can be made based on certain field values in a QlikView document. When entering field values in *Section Access* connecting to field values in *Section Application*, it is very important that all values really exists in the section application. If this is not the case, and you log in using a value that exists only in section access, no reduction will take place (if using QlikView 7.01 or earlier). This is due to the associative logic in QlikView. If no value is found, no selection will be made and hence no reduction will take place.

To be absolutely sure that there is no discrepancy between the fields you can load the field from section access separately into section application.

2.3. Example of using Section Access for Data Reduction

In the following example an Excel spreadsheet has been used to define the user database, and to store the matrix that will later be used for the reduction and hiding objects.

2.4. The user database

The user-database in Excel is the simplest form of authentication used by QlikView. To be able to make the example below, you have to create an Excel spreadsheet containing the following data:

USERID	PASSWORD	ACCESS	GROUP
ADMIN	123	ADMIN	
B	123	USER	GROUP1
C	123	USER	GROUP2
D	123	USER	GROUP3
E	123	USER	GROUP4

Users are authenticated by using USERID and PASSWORD. The ACCESS field indicates if the user has Admin or User access to the QlikView document. The field GROUP is used for data reduction. This field is empty for the ADMIN user, preventing any data reduction to occur and therefore making all data available for this user.

2.5. Applying the user database

1. Start QlikView and open a new document (*Folder – New*).

2. Enter the script menu and use the table wizard to generate the load statement loading data from the Excel spreadsheet. You will have the following in the script once you exit the wizard:

```
Directory;
Load
     [USERID], [PASSWORD], [ACCESS], [GROUP]
FROM security.xls (biff, embedded labels, table is
[Users$]);
```

3. Add the Section Access statement to the script, to define the Section Access part of the script. End the Section Access entering Section Application:

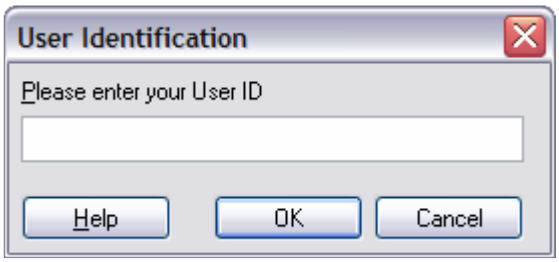
```
Section Access; // Start of section access part

Directory;
Load
     [USERID], [PASSWORD], [ACCESS], [GROUP]
FROM security.xls (biff, embedded labels, table is
[Users$]);

Section Application; // End of section access part
```

4. Reload your script and save your QlikView document.

Information stored in Section Access of the QlikView document will not be visible inside the script. However the information will be used for authentication next time the QlikView document is opened.

5. Close QlikView and start it again (this is to make sure that the User cache is empty when opening your secured document).

6. Open your saved QlikView document. Note that you now have to login by entering UserID and Password to be able to access the document.



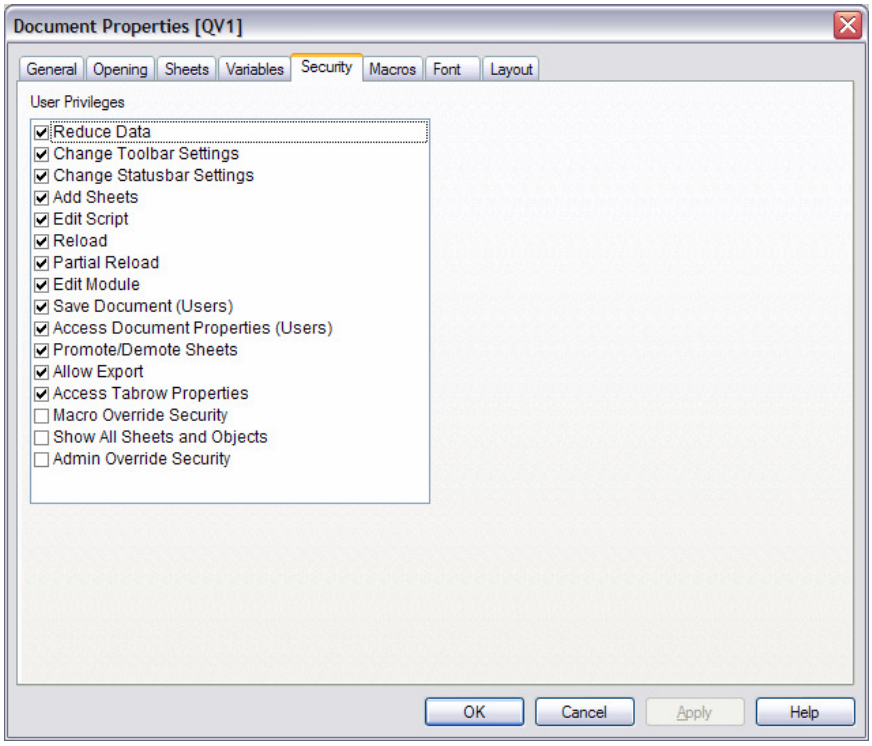
7. Log in using UserID: Admin, Password: 123. Remember, the UserID and password were stored in security.xls, and this login example assumes you created the specified login credentials.

2.6. Access restrictions in QlikView

The “Admin” in our database has Administration rights on the QlikView document. It is possible for an Admin to limit the functionality for users with User rights in QlikView. For example, the Admin can restrict users from being able to save the document, access the script, and so on.

2.7. Security on the document level

The security settings on the document level can be found in *Settings – Document Properties – Security*:



2.8. Limit access for the users

1. Open the **Security** page on the **Document Properties** level

2. Uncheck **Reload** and **Save Document (Users)** to prohibit the users from being able to reload or save the document. Also uncheck **Edit script**.

3. Press **OK** to close the dialog.

Note! You will no longer be able to access the script dialog. As an admin you want to be able to override the security settings for the users:

4. Open the **Security** page again and check **Admin Override Security** to have full functionality once logged in as an admin.

5. Press **OK** to close the dialog.

6. Save your document and close down QlikView (to clear the logged in user from the cache).

7. Open QlikView and your saved document, but this time log in using:
   - UserID: B
   - Password: 123.

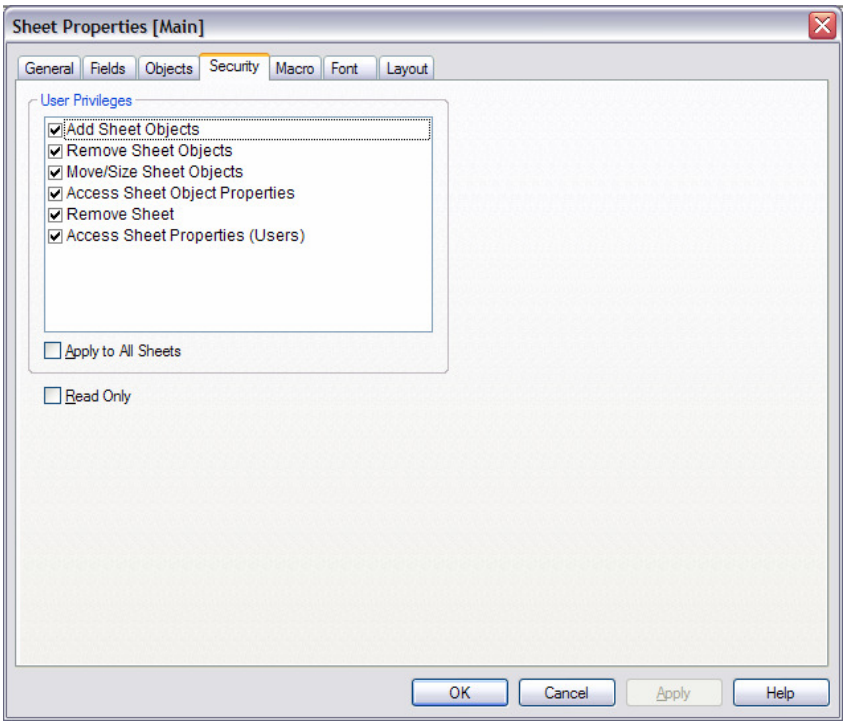
8. Notice that you will not be able to access the script or to reload/save the document.

9. Quit and login using the admin-account (UserID:Admin, Password:123).

Note! The Security page on *Settings – Document Properties* will only be available for users logged in as "Admin"!

2.9. Security on the sheet level

In the same ways as you can define the security on the document level, it is possible to set the security settings on the sheet level. This is done using the Security page on Settings – Sheet Properties:



3. Example of how to prevent discrepancy in fields in data reduction (prior to QlikView 7.01)

In QlikView 7.01 and above, the function “Strict Exclusion” has been added to prevent non authorized users from having access to reduced data. In versions prior to QlikView 7.01 there is a work-around to solve this problem.
Below you find an example of a basic use of Section Access for data reduction on Open Document.

We have a table named Employees:

EmployeeNo	Name	Department
1	Bill	A
2	Bob	A
3	Ann	A
4	Jill	A

This is what the Script looks like:

```
Section access;

Load * Inline [
UserID,Access,Department
x,admin,A
y,user,B
];

Section application;

SQL SELECT
EmployeeNo,
Name,
Department as DEPARTMENT
FROM Employees;
```

The table only contains employees working in department A. According to Section Access, User Y shall only be able to see data related to department B. However, department B does not exist in the Employees table and this results in no data reduction, hence User Y will see all data. The most likely scenario is for User Y to see no data at all. To avoid this from happening, all possible departments have to be read into the Employees table, even if they contain no data.

A *Load Inline table* is added resulting in the following script:

```
Section application;

SQL SELECT
EmployeeNo,
Name,
Department as DEPARTMENT
FROM Employees;

Load * Inline [
DEPARTMENT
A,
B
];
```

By adding the Inline table, a dynamic reduction will be made based on the field Department, even if User Y logs in.

3.1 The data reduction matrix

Once the authentication model is implemented, it is possible to control what part of the QlikView document that should be accessible for each user. In our example this is controlled by assigning each user to a group, using the field GROUP in *Section Access*.

Note! This field is not a reserved field in *Section Access*, but is used to link each user from section access to a field value in *Section Application*.

3.2. Adding the reduction matrix

The matrix below describes what parts of the QlikView document that should be visible to different users. To be able to make the example below, you have to create an Excel spreadsheet containing the following data:

GROUP	SHEET1	SHEET2	SHEET3
GROUP1	1	1	1
GROUP2	0	1	1
GROUP3	0	0	1
GROUP4	1	0	1

The field GROUP is the link to the users in section access. SHEET1-3 are used later when applying the function show/hide to different sheets.

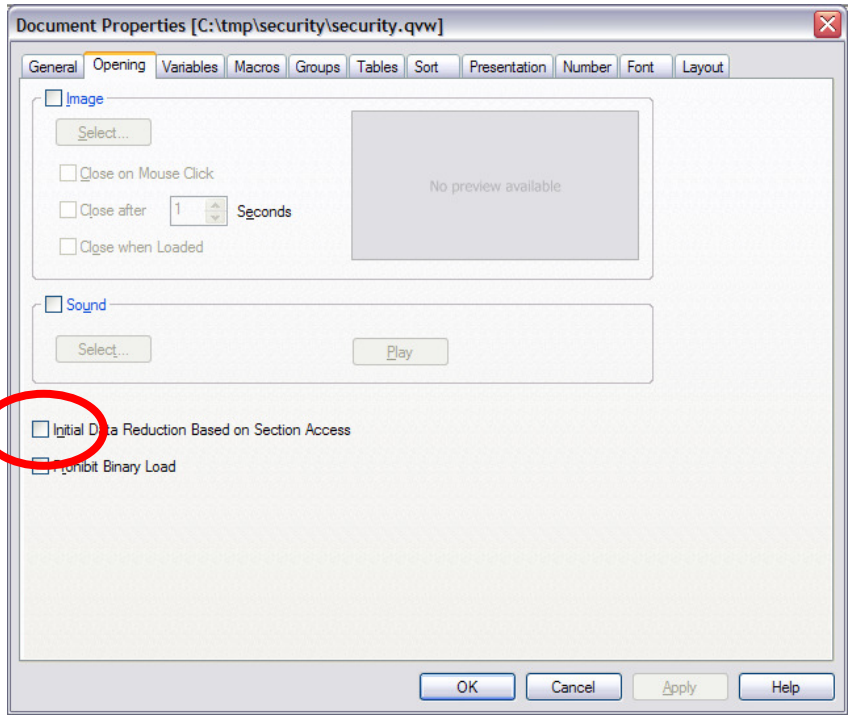
1. Open your QlikView document that contains the section access script created above. Log in using UserID: Admin, and Password: 123.
2. Enter the script dialog. Make sure the cursor is placed after the *Section Application* statement and use the table wizard to add the matrix that should be used to control the sheet access for different users. **Be sure to select the Matrix sheet using the Table button.** Your script should now look like the this:

```
Section access;
Directory;
Load
     [USERID], [PASSWORD], [ACCESS], [GROUP]
FROM security.xls (biff, embedded labels, table is
[Users$]);

Section application;

Directory;
Load
     [GROUP], SHEET1, SHEET2, SHEET3
FROM security.xls (biff, embedded labels, table is
[Matrix$]);
```

3. Reload the script.

4. Add the fields SHEET1-3 to your application. Notice that all values will be available in the fields. When making a reload, all values are retrieved from the database.

5. For QlikView to be able to reduce the information in the document, you must activate *Initial Data Reduction Based on Section Access*. This is done in **Document Properties – Opening**.



6. Save the document and close down QlikView.

7. Open the document again and log in as UserID:B with Password:123. The fields SHEET1-3 should now only contain 1's.

8. Try to log in using another user to verify that the information in the three fields will change for each user.

3.3. Applying the matrix to the sheets

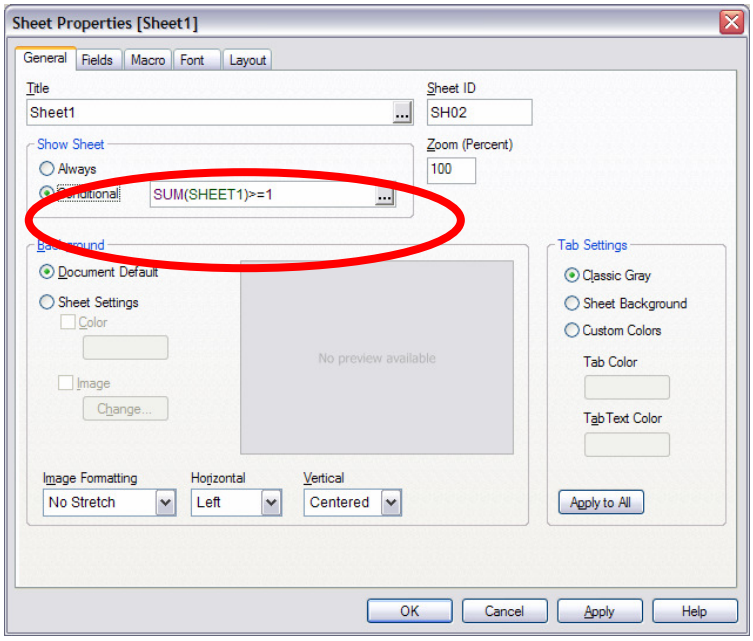
When the authentication model is working and the matrix is connected to each user, the values in the fields SHEET1-3 are used to show and hide different sheets based on the user logged in.

1. Open the QlikView document and log in as User: Admin, and Password: 123.

2. Add three new sheets in your QlikView-document.

3. Access the sheet properties for the first sheet by right-clicking on the sheet and select **Properties.**

4. On the **General** page, locate the **Show Sheet** section and select **Conditional**. Add the expression Sum(SHEET1)>=1 as shown below:



5. Do the same for the other sheets, but instead use Sum(SHEET2) and Sum(SHEET3) in the expression.

   We use Sum(SHEET1) etc and not only an expression saying SHEET1=1 because when we reload the document, all values in the field SHEET1 will be available (0,1). The expression SHEET1=1 will only be true when SHEET1 only contains the value 1. This means that the sheet would disappear on a reload.

6. Save and close your QlikView document.

7. Open QlikView and the previously saved document. Log in with User:C and Password: 123. User C does not have access to the first sheet (SHEET1). User C is included in GROUP2. According to the matrix, GROUP2 only has access to SHEET2 and SHEET3.

4. Applying NT Security in Section Access

QlikView can be integrated with Microsoft Windows NT security, making single sign-on possible when connected to a Windows NT Domain. By using NT security, the user won't need to log into a secured QlikView file. Instead the information for authentication is retrieved from the operating system (Microsoft Windows).

4.1. Fields used for applying NT security in Section Access

The specific fields for NT security used in Section Access are NTNAME, NTDOMAINSID and NTSID.

NTNAME: A field that contains a string corresponding to a *Windows NT Domain User Name* or a *Windows NT Group Name*.

NTDOMAINSID: A field that contains a string corresponding to a Windows NT Domain SID. This is a unique string identifying a specific Domain.

NTSID: A field that contains a Windows NT SID. An NTSID is a combination of the NT Domain SID and a unique identifier for the NT User or Group.

You can use one of the fields or a combination to log on to the QlikView document. The most common combination is to use the NTDOMAINSID to get the unique identifier for the domain and combine it with NTNAME to get the unique users for this domain.

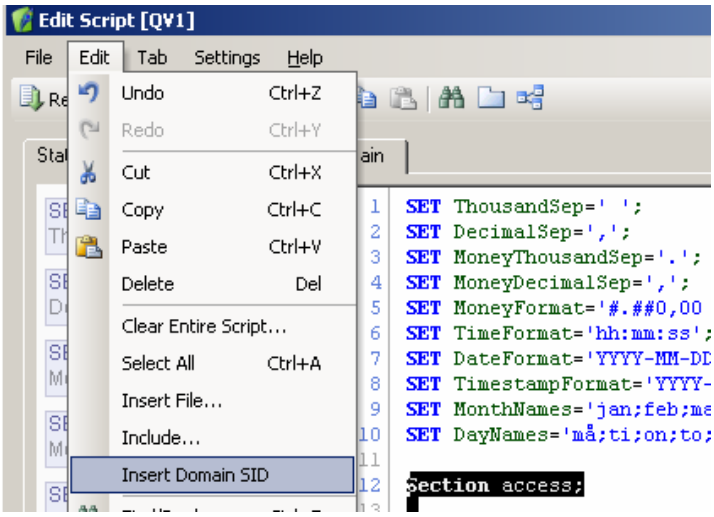
If you have NT security in the QlikView document, QlikView will check your logged in information from the operating system and match this information with the information stored in the QlikView file. If the information matches you will have access and QlikView allows you to log on to the document.

4.2. How to use NTDOMAINSID and NTNAME in Section Access

The easiest way to define and use NT-SID's in Section Access is to use the NTDOMAINSID and the NTNAME:

USERID	PASSWORD	SERIAL	NTNAME	NTDOMAINSID	NTSID	ACCESS
		*	BMW	S-1-5-21-2069525358-1535916410-466756119	*	ADMIN

The NTDOMAINSID can be retrieved using "Insert DomainSID" from the Script Editor – Edit.



NTNAME is the username used to identify the user on the network. In the example above only user BMW with the DomainSID S-1-5-21-2069525358-1535916410-466756119 will gain access to the file.

Note! *Make sure that the values in field USERID and PASSWORD are NULL and not an empty string. When reading from Excel spreadsheets, the* ***trim****()-function should be used because an empty cell in Excel is considered as an empty string and not a NULL-value:*

```
Section access;
Directory;
Load
     trim([USERID]) as [USERID],
     trim([PASSWORD]) as [PASSWORD],
     SERIAL, NTNAME, NTDOMAINSID, NTSID, [ACCESS]
FROM security.xls (biff, embedded labels, table is
[Users$]);
```

NTNAME can also include a group-name. In this example, all Domain Administrators on the Domain will have access to the file:

USERID	PASSWORD	SERIAL	NTNAME	NTDOMAINSID	NTSID	ACCESS
		*	ADMINISTRATORS	S-1-5-21-2069525358-1535916410-466756119	*	ADMIN

4.3. Combining NT Security and QlikView's built-in security

If you want to work with a QlikView document both on and off line, you have to use both QlikView's built-in security and NT Security. To do so, you have to create a table consisting of both the fields you want to use in the NT Security, and the fields you want to use for the QlikView Security. The two kinds of security must be placed on two different rows for each user:

USERID	PASSWORD	SERIAL	NTNAME	NTDOMAINSID	NTSID	ACCESS
		*	BMW	S-1-5-21-2069525358-1535916410-466756119	*	ADMIN
A	123	*	*	*	*	ADMIN

In the example above, the user BMW is logged in using NT Authentication when connected to the network. If no NTNAME/Domain is found (ie, not connected to the network), the user is prompted to use UserID and Password for identification (A/123 in this example).

One common mistake is to put this information on the same row like:

USERID	PASSWORD	SERIAL	NTNAME	NTDOMAINSID	NTSID	ACCESS
A	123	*	BMW	S-1-5-21-2069525358-1535916410-466756119	*	ADMIN

In this case the user must both be connected to the network ***and*** use UserID/Password for identification.

Note! The NT security only works if you are logged on to the network. You cannot use NT security while off line.

4.5. Batch load

When refreshing a QlikView document using batch-files / scheduled reload, you must be aware that the scheduler may be running with an account other than your personal network account. It is therefore not recommended to use NT-Authentication when loading QlikView documents in batch but instead add a specific user in Section Access for this task. This user should only be identified using SERIAL. By doing this you don't have to worry about SID's, UserID/Password etc:

USERID	PASSWORD	SERIAL	NTNAME	NTDOMAINSID	NTSID	ACCESS
		4600 9999 9999 9999	*	*	*	ADMIN

5. Binary load of document with Section Access

If you make a Binary load of a QlikView document (document A) containing Section Access, the security will be applied on the new document (document B). However, if you add a separate Section Access in document B, there will be no heritage of security setting from document A.

When making a binary load of a document with Section Access, the UserID and Password must be provided once the script is executed. When running a Batch load, this login procedure must be avoided. The solution is to add the serial number of the QlikView running on the server (4600 9999 9999 9999 in the example below) in the Section Access of both applications.

5.1 Example of Batch load script

Section Access for document A:

```
Section access;

Load * Inline [
UserID,Password,Access,Serial
,,ADMIN,4600 9999 9999 9999
admin,admin,ADMIN,*
];
```

Section Access for document B

```
Section access;

Load * Inline [
UserID,Password,Access,Serial
,,ADMIN,4600 9999 9999 9999
x,y,USER,*
];
:
```