Author	**ALH, BMW, HBE, LJN**	Create date	**02-Dec-03**
Project	**Section Access in QlikView**	Last save date	**4-Dec-03**
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 of how data protection and security are 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 are set in the script. Access rights and User Levels are defined in the *Section Access* part of the script. The 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.

1.2. Section Access system fields

The 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 e.g. 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 e.g. serial number only.

- **ACCESS** A field that defines what access the user should have.
- **USERID** A field that should contain a user ID that has the privilege specified in the field ACCESS.
- **PASSWORD** A field that should contain an accepted password.
- **SERIAL** A field that should contain a number corresponding to the QlikView serial number. Example: 4900 2394 7113 7304

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

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

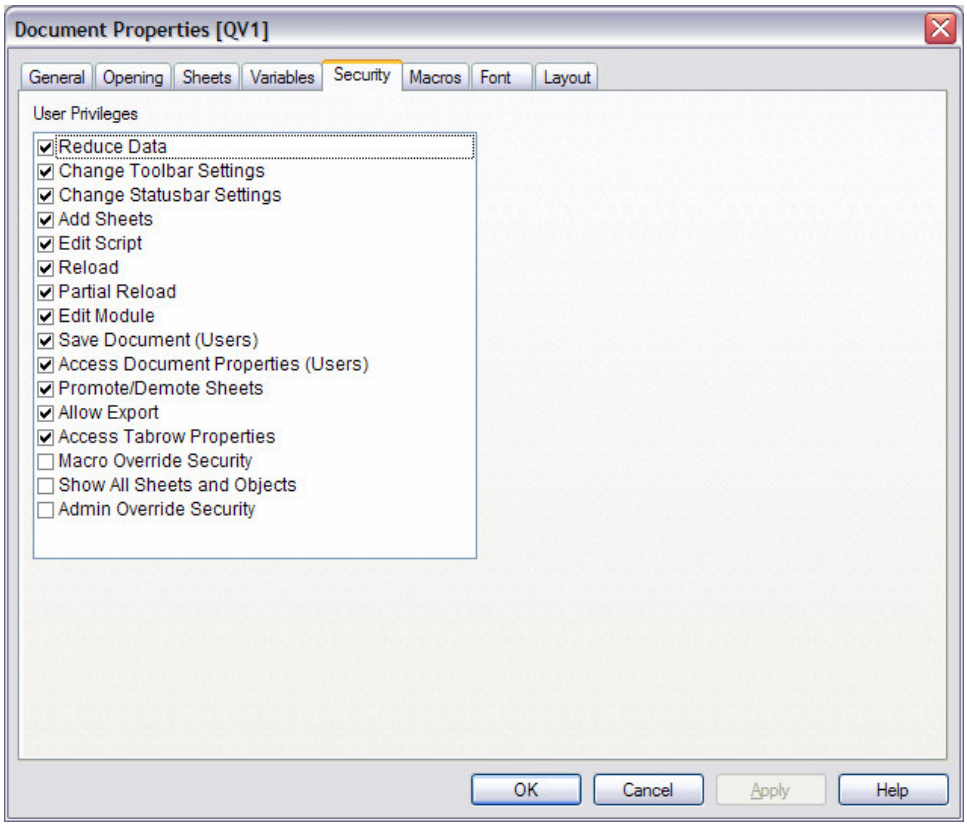
- **NTSID** A field that should contain a Windows NT SID. Example: S-1-5-21-125976590-467238106-1092489882-1378

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,* Part IV, Chapter 22.

1.3. User levels

There are basically three different access levels to a QlikVeiw document. These are ADMIN, USER and NONE. ADMIN will give the person logging in access to every part of the document including the Security tabs located in the *User Preferences, Document Properties* 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 userids 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 written it in the Section Access, it will be changed to upper case by QlikView when a user tries to log in.

2. Data reduction on Open Document

In QlikView data can be reduced based on the login when opening a document. This method was originally developed for QlikView Server, but can also be used in stand alone QlikView. It's called "Reduction based on Section Access". This method could be useful to prevent salesmen to have access to other salesmen's information or to prevent employees from viewing 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 mark *Prohibit binary Load* on the same tab.

Note! A reduced document should never be allowed to be saved under the same name (The document would then only hold a subset of values). Users should never be allowed to run the script since this would load all data into the application. This is prevented by marking 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 the QlikView document. When entering field values in *Section Access* connecting to field values in *Section Application*, it is very important that all values really exist 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. 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.

If you want to give a user or an administrator access to all values, you will have to specify this in section application. You have to use the star (*) to show all the values and then you have to put the string Star is * in 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 / hide 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 will be authenticated using UserID / Password. The Access field will tell if the user will have Admin or User access to the QlikView document. The field Group will be used for the data reduction.

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 for loading data from the Excel spreadsheet. The script should read as follows:

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

3. Add the Section Access statement to the script ending with the Section Application statement:

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

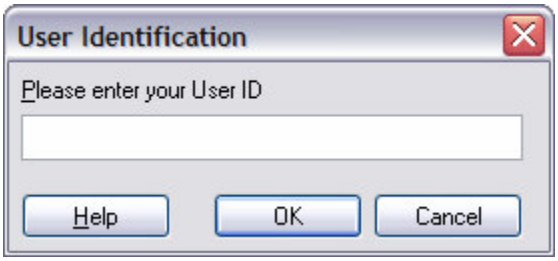
```
Directory;
Load
     [USERID], [PASSWORD], [ACCESS], [GROUP]
FROM security.xls (biff, embedded labels, table is
[Users$]);

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.



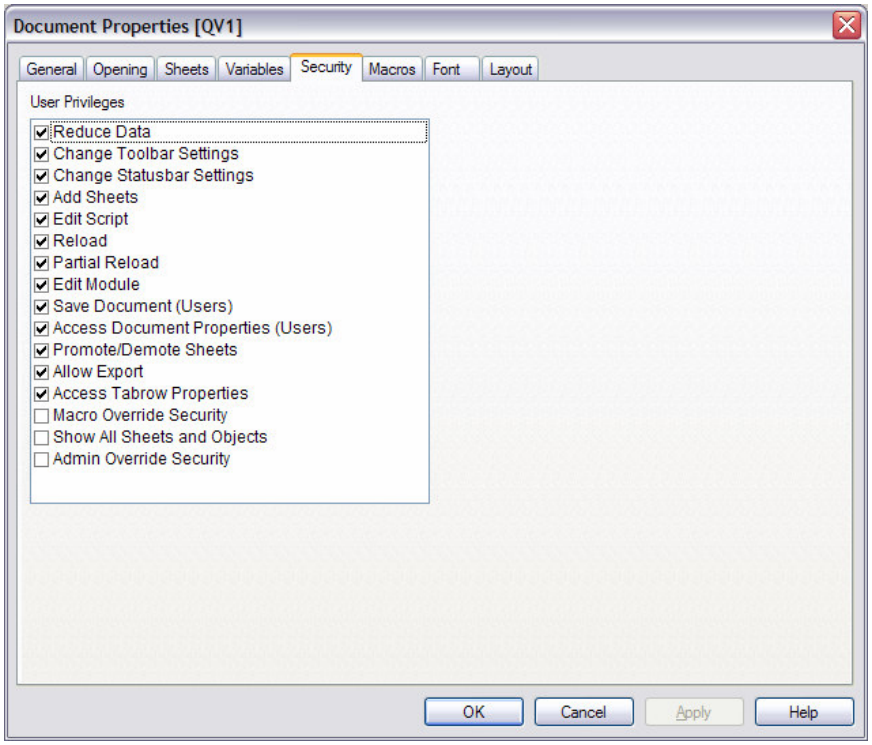
7. Log in using UserID: Admin, Password: 123.

2.6. Access restrictions in QlikView

The “Admin” in our database will have Administration rights of 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** tab on the **Document Properties** dialog.

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! that 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.

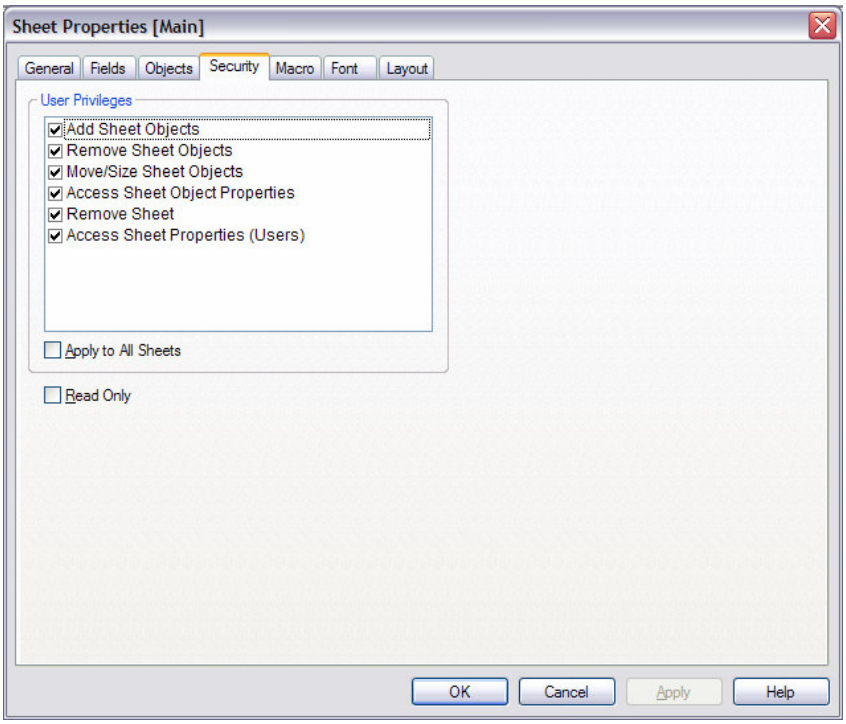
8. Notice that you will not be able to access the script or to reload/save the document.

9. Quit and log in 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

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 se 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 to happen, all possible departments has to be read into the Employees table, even if they hold 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 used to link each user from section access to a field value in *Section Application*.

3.2. Adding the reduction matrix

The matrix describes what parts of the QlikView document 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 will be 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, Password: 123.
2. Enter the script dialog. Make sure that 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:

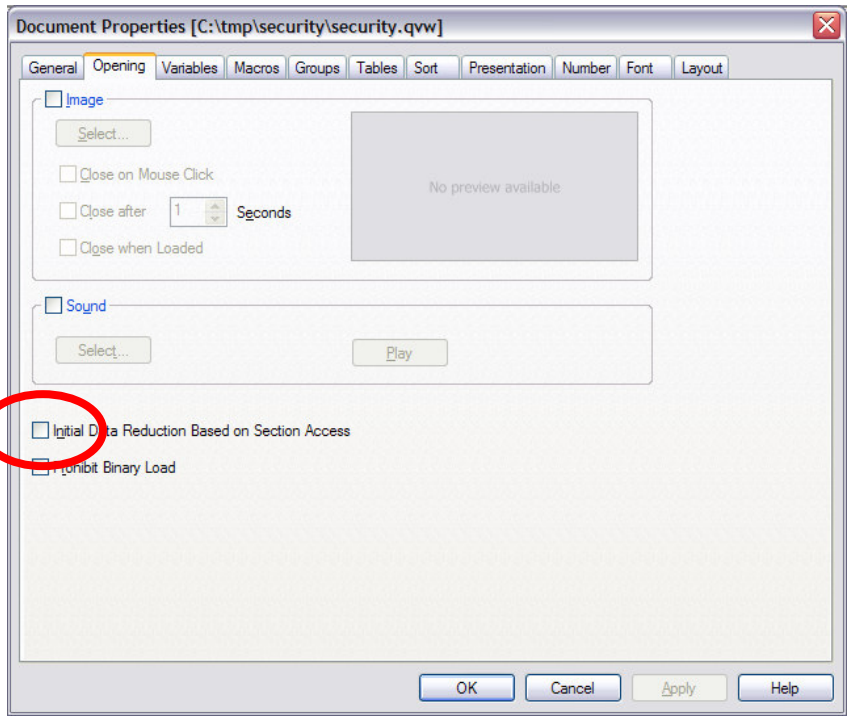
```
Section access;
Directory;
Load
     [USERID], [PASSWORD], [ACCESS], [GROUP]
```

```
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

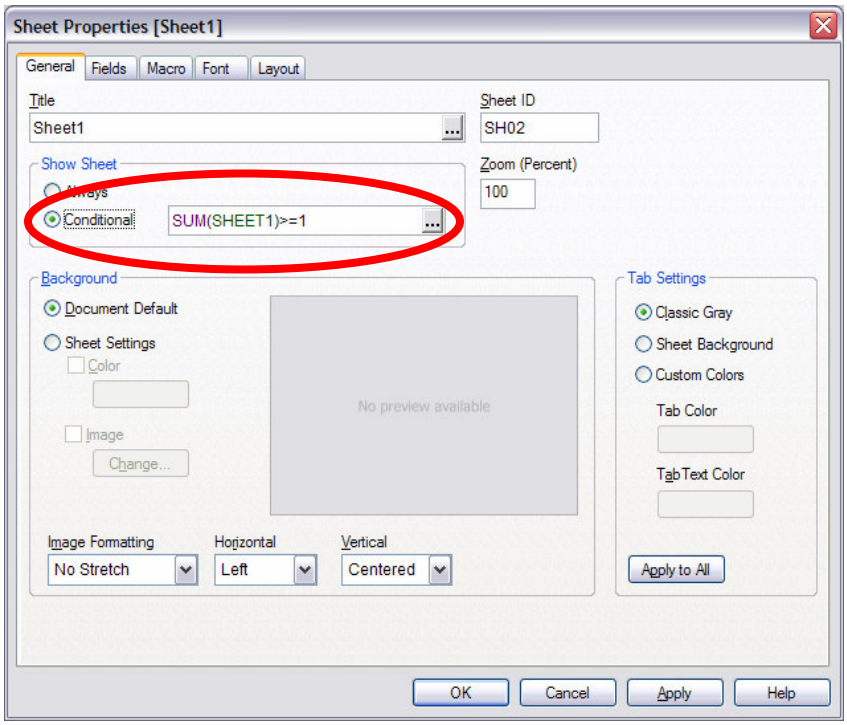
When the authentication model is working and the matrix has been connected to the users, the values in the fields SHEET1-3 can be used to show and hide different sheets depending on who is logged in.

1. Open the QlikView document and log in as User: Admin, 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 on the other sheets, but use Sum(SHEET2) and Sum(SHEET3) in the expression instead.

   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 your document and close down QlikView.

7. Open QlikView and the previously saved document. Log in with User:C and Password: 123.

Note! User C will not have access to the first sheet (SHEET1). User C will be included in GROUP2, and according to the matrix, GROUP2 will only have 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. By using NT security the user won't need to log into a secured QlikView file. Instead the information for authentication will be 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 should contain a string corresponding to a *Windows NT Domain User Name* or a *Windows NT Group Name*.

NTDOMAINSID: A field that should contain a string corresponding to a Windows NT Domain SID. This is a unique string that identifies a specific Domain.

NTSID: A field that should contain 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-SIDs 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. Notice that the other fields, (if defined in Section Access), must be set to (*).

NTNAME can also include a group-name. In this example, all 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 be able to work with a QlikView document both on and off line, you will have to use both QlikView's built-in security and NT Security. If so, you have to create a table consisting both of the fields you want to use in the NT Security, and the fields you want to use for the QlikView Security. The two different 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 will be logged in using NT Authentication when connected to the network. If no NTNAME/Domain can be found (ie, not connected to the network), the user will be 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:

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.

4.4. Considerations when using NT Security in QlikView

The implementation of integrated NT Security is much the same as general security implementation in QlikView. However, there are some things to consider:

4.5. Batch load

When refreshing a QlikView document using batch-files (scheduled reload), you must verify that the scheduler is running on a different account than your personal network account. A recommendation when loading QlikView documents in batch is to 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 SIDs, UserID/Password etc:

USERID	PASSWORD	SERIAL	NTNAME	NTDOMAINSID	NTSID	ACCESS
*	*	4600 2394 7111 8018	*	*	*	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,*
];
:
```