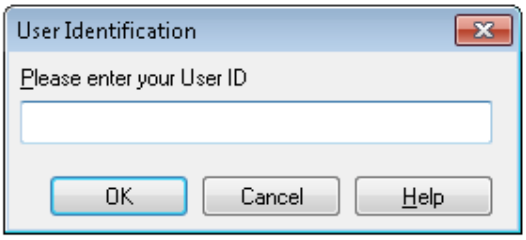
QlikView

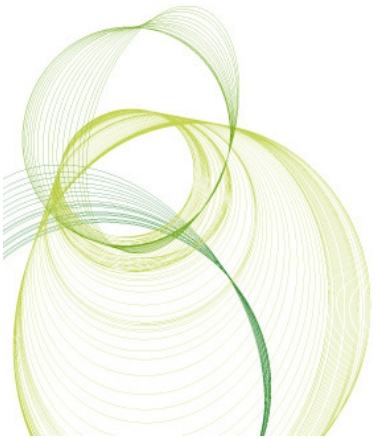
Introduction to Section Access



Gustav Guldberg
QlikTech Inc

Revision 1 - 2010 June 08

2010 April 17



About this document

This document serves a compliment to the information on Section Access in the QlikView Reference Manual and is aimed towards users who are new to Section Access, to use it in addition to the Developer training and reference manual or just to brush up on old knowledge.
The examples are designed for QlikView Developer 9 but the script will work in QlikView Developer 8.50 SR3 and later.

**Note that this document does not cover the usage of Section Access for the thin clients (Plugin, Java and Ajax) or reloads via QlikView Publisher 8.50.x or QlikView Server (Enterprise) Management console in 9.00.x. These topics will be covered in an upcoming guide and more advanced Section Access solutions.

Words of Warning

- Before implementing Section Access in your document, backup your application. Incorrect syntax will render your document inaccessible and there's no possibility of recovering the data or script.

- It is good practice to work with multiple copies of the document to be able to revert back to an earlier document in case an error is made in the script.

Table of Contents

Why use Section Access?

There are two good reasons to implement section access into your documents.

- To help protect your data from unauthorized access.
- To limit what data authorized users can see and what they can do.

QlikView is a great way to gather information and enable easy analysis of data. However a QVW document, like any other computer file might get lost or stolen. A QVW file without Section Access can be opened by anyone that has QlikView installed and this might put your data at risk and a document with section access properly implemented can't.

There are also scenarios where you don't want authorized users to view the full data set. Section Access does a great job in reducing data to control what authorized user can see and cannot see.

Section Access comes in many flavours. A simple username and password might be sufficient for some documents where in other scenarios you want a specific user to sit inside your domain and be logged in as a specific user to a specific machine and use a certain serial number. Section Access can do this too.

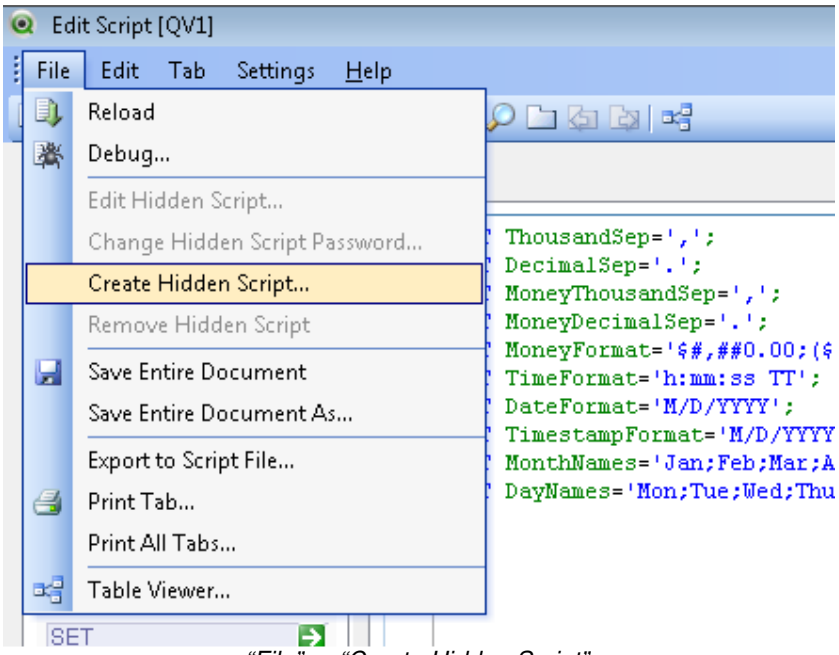
How to setup and enable Section Access

Setting up a working Section Access solution is done in three steps.

Designing the Section Access definition in the script
Enabling Section Access on document level and define the user permissions
Set the USER level access

Hidden Script

When implementing Section Access it is advisable to do so in the hidden script.



"File" -> "Create Hidden Script"

Since the user credentials will be displayed in clear text (if using inline data) or the location of the Section Access definitions, all users with ADMIN status will be able to see the script as well as users given the privilege to see the script. If the Section Access solution is created in the hidden script it further ensures data security. Keep the hidden script password in a safe place since this password cannot be recovered if lost. The same goes for the ADMIN password, if you lose this password access to the document will be denied and there is no way to recover the password.

Access Control

All access control can be managed via text files, databases or INLINE clauses in the same way as data is normally handled by QlikView.
The ACCESS section is loaded in the script is declared by the statement, SECTION ACCESS;.
The SECTION ACCESS declaration should be defined before the actual data is added for SECTION APPLICATION.

Section Access System Fields

The access levels are assigned to users in one or several tables loaded within section access. These tables can contain several different user-specific system fields.
One can combine several of the fields listed below to build the Section Access solution depending on the desired level of security.
Apart from the standard fields, additional fields can be defined to administer data reduction for each user.

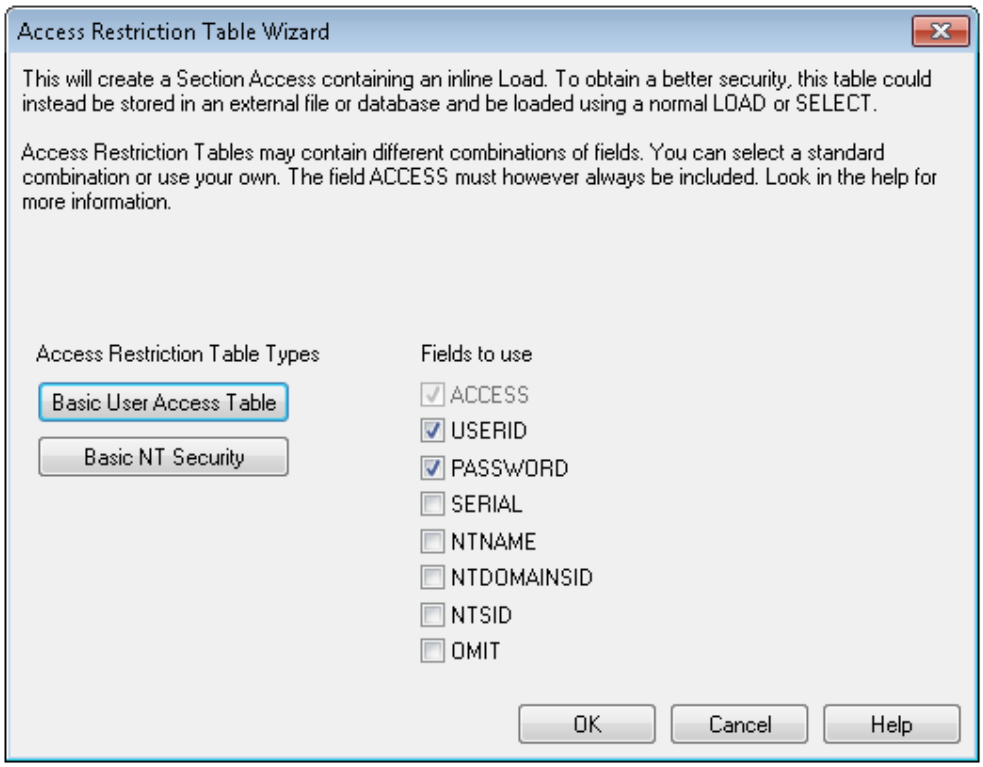
**Note that all data loaded via an external data source must be loaded in upper case in the SECTION ACCESS statement. This does not apply to INLINE data which always will be treated as upper case.

Example:

```
SECTION ACCESS;
LOAD
        UPPER(Level) AS ACCESS,
        UPPER(DomainName) AS NTNAME,
        UPPER(PASSWORD) AS PASSWORD
FROM Access.XLSX;

SECTION APPLICATION;
```

Field used in the script for Section Access



"Data" -> "Inline Data" -> "User Access"

ACCESS

A field that defines what access the corresponding user should have and is a required field for all section access solutions.
There are two access levels in Section Access, "ADMIN" and "USER". The ADMIN controls what the USER can see and do in the QlikView document. An individual with ADMIN privileges can change everything in the document.
(A user opening a document via QlikView (Open in Server), Plugin, Java or Ajax client will always have USER status, regardless of the definition in ACCESS).

USERID

A field that should contain an accepted user ID.
QlikView will prompt for a User ID and compare to the value in this field.
This user ID is not the same as the Windows user ID.
Note that the USERID isn't case sensitive. All fields in the Section Access definition is interpreted as uppercase.

PASSWORD

This field must contain an accepted password.
QlikView will prompt for a Password and compare to the value in this field.
This password is not the same as the Windows password.
Note that the USERID isn't case sensitive. All fields in the Section Access definition is interpreted as uppercase.

SERIAL

This field must contain a number corresponding to the
QlikView serial number.
Example: 4900 2394 7113 7304.
QlikView will check the serial number of the user and compare it to the value in this field.
The SERIAL can be found in QlikView, "Settings"->"User Preferences"->License-tab.

NTNAME

This field must contain a string corresponding to a Windows
NT Domain user name or group name.
QlikView will fetch the logon information from the OS and compare it to the value in this field.
Example: DOMAIN\NTNAME

NTDOMAINSID

This field must contain a string corresponding to a Windows NT Domain SID.
Example: S-1-5-21-125976590-467238106-1092489882
QlikView will fetch the logon information from the OS and compare it to the value in this field.
The NTDOMAINSID can be derived from the script, "Edit"->"Insert Domain SID"

NTSID

This field must contain a Windows NT SID.
Example: S-1-5-21-125976590-467238106-1092489882-1378
QlikView will fetch the logon information from the OS and compare it to the value in this field.
The NTSID can be generated via free 3'rd party applications such as "Getsid.exe".

OMIT

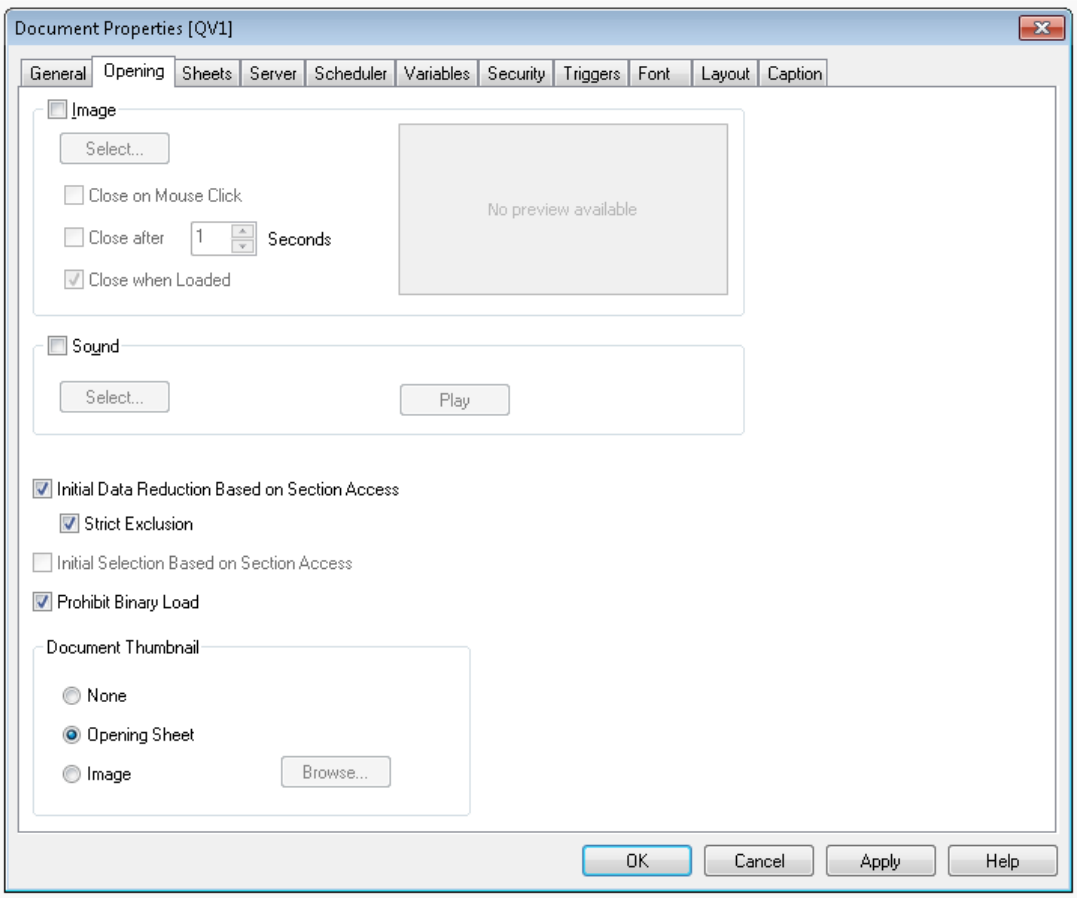
A field that should be omitted for a specific user.

REDUCTION

A reduction field can be added to control access to data for each individual user.
The value in the reduction field is used to match against another field in the application with same name. If a match is found, the data will be reduced for the field and presented to the user. The result will be the same as if this field was selected in the application and all none associated fields would be reduced.

If the section access solution contains more than one reduction field the logic was made stricter in the SR3 release of 8.50.
If the two (or more) reductions are mutually exclusive and "Strict Exclusion" is used, QlikView will refuse to open the application. I.e. there may be applications that you can open with previous versions, but not with QlikView 8.50 SR3.

Define Section Access on document level



"Settings" -> "Document Properties" -> "Opening"

"Initial Data Reduction Based on Section Access"

Tick the checkbox to enable section access in the document.

“Strict Exclusion”

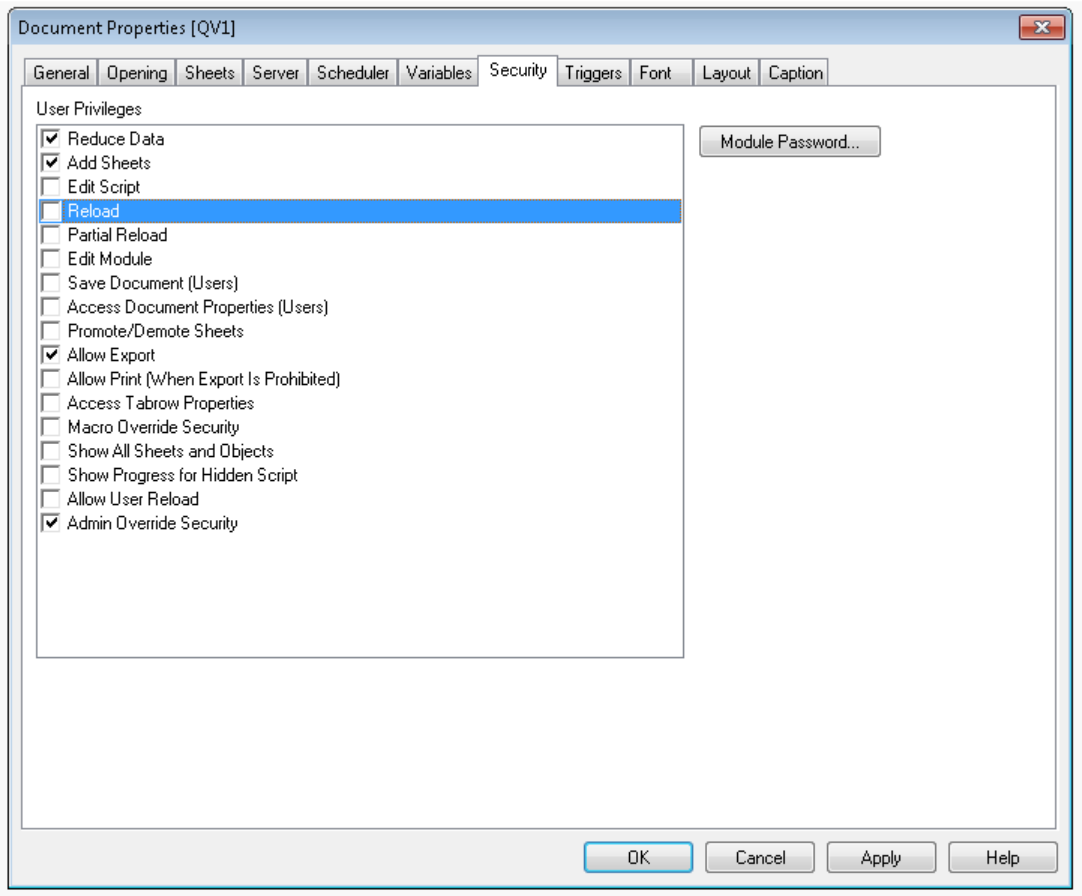
Access to the document will be denied whenever the field values in the section access reduction fields lack matches in their corresponding section application field.
Having this option unselected will mean that if QlikView can’t find a match to reduce data, all data in the document will be visible on USER level. However, ADMIN will always be able to see all data, regardless of the reduction. Best practice is to use strict exclusion to avoid unwanted access to the QlikView document.

“Prohibit Binary Load”

If this option is selected it will not be possible to load data from the document’s qvw file via a binary statement in another QlikView document. It’s highly recommended to use this option to increase security.

Security Settings on Document Level

In the security tab, one can define what actions a user with USER privileges can perform.
It's of great importance to define the appropriate settings in this tab since giving a USER too many privileges can render the security implementation useless.
If you with to have a clear distinction between ADMIN and USER, review these settings.
Do note that the security-tab is only accessible by an ADMIN in the section access solution.



"*Settings" -> "Document Properties" -> "Security*"

Reduce Data

If this check box is left unchecked, the Reduce Data command in the File menu becomes inactive.

Add Sheets

If this check box is left unchecked, the Add Sheet command in the layout menu becomes inactive.

Edit Script

If this check box is deselected, the Edit Script command in the File and in the toolbar becomes inactive.

Reload

If this check box is deselected, the Reload command in the File Menu and in the toolbar becomes inactive.
Since a reload of a document always will result in a full data set, it's not advisable to let a user reload a document.

Partial Reload

If this check box is deselected, the Partial Reload command in the File menu becomes inactive. Since a reload of a document always will result in a full data set, it's not advisable to let a user reload a document.

Edit Module

If this check box is deselected, the Edit Module command in the File menu becomes inactive.

Save Document (Users)

If this check box is deselected, the Save command in the File menu becomes inactive for persons with USER privileges.
If a user is allowed to save, a reduced data set might be saved thus locking other users out of the document.

Access Document Properties (Users)

If this check box is deselected, the Document Properties command in the Settings menu becomes inactive for persons with USER privileges.
Note that a USER will never be able to see the "Opening" and "Security" tabs even if this option is selected.

Promote/Demote Sheets

If this check box is deselected the Promote Sheet and Demote sheet commands in the Layout menu become inactive.

Allow Export

If this check box is deselected all Export, Print and Copy to Clipboard commands become unavailable.

Allow Print (When Export Is Prohibited)

Although the check box Allow Export above is deselected all Print commands remain available if this check box is selected.

Access Tabrow Properties

If this check box is deselected the Tabrow Properties (see page 85) can no longer be accessed.

Macro Override Security

If this check box is selected, it is possible to override all security settings by means of macros and commands via the Automation API.

Show All Sheets and Objects

If this check box is selected all conditional display of sheets and sheet objects is overruled, so that all sheets and sheet objects become visible. This functionality can be toggled by pressing CTRL+SHIFT+S.

Show Progress for Hidden Script

If this check box is selected the script progress dialog will be shown while executing the script.

Allow User Reload

If this check box is deselected it will not be possible to reload the script when the document is opened in USER mode, even if the Reload check box above is selected..

Admin Override Security

If this check box is selected all security settings for the document and sheets will be disregarded while in ADMIN mode.

Examples of different security implementations:

The following are a few common examples of implementations of Section Access with different levels of security. Bear in mind that adding NTNAME, NTDOMAINSID and NTSID will make the authentication process take longer because QlikView must find this information and verify before access can be granted.

A common misconception in section access is the use of "*" (star) in section access. "Star" means "all listed values" not all values for the field. This will be explained in detail in the script examples.

Example 1:

```
Section Access;
LOAD * INLINE [
   ACCESS,     USERID,      PASSWORD
   ADMIN,      ADMIN,       ADMIN
   USER,       USER1,       U1
   USER,       USER2,       U2
   USER,       USER3,       U3
];
```

This is a very basic form of authentication.
The document can be opened from anywhere and the only thing required is the knowledge of the USERID and PASSWORD to gain access. Not a very safe from a security standpoint. The authenticated user will be able to see all data in the application.

Example 2:

```
Section Access;
LOAD * INLINE [
   ACCESS,     NTNAME,              PASSWORD
   ADMIN,      DOMAIN\ADMIN,        ADMIN
   USER,       DOMAIN\USER1,        U1
   USER,       DOMAIN\USER2,        U2
   USER,       DOMAIN\USER3,        U3
];
```

This is more secure and requires the user to be logged in with the NT-account and have knowledge about the password. The advantage of this is that no USERID is required.

Example 3:

```
Section Access;
LOAD * INLINE [
   ACCESS,     NTNAME,              PASSWORD,   SERIAL
   ADMIN,      DOMAIN\ADMIN,        ADMIN,
   USER,       DOMAIN\USER1,        U1,         1234 5678 9012 3456
   USER,       DOMAIN\USER2,        U2,         2345 6789 0123 4567
   USER,       DOMAIN\USER3,        U3,         3456 7890 1234 5678
];
```

This example is more secure since it requires the user to open the document from a copy of QlikView that has been registered with the listed license number.

Example 4:

```
Section Access;
LOAD * INLINE [
   ACCESS,     NTNAME,        PASSWORD,   SERIAL,                NTSID
   ADMIN,      DOMAIN\ADMIN,  ADMIN,                ,
         *
   USER,       DOMAIN\USER1,  U1,         1234 5678 9012 3456,  S-1-
5-21-2068569857-8585916410-466756119-12345

   USER,       DOMAIN\USER2,  U2,         2345 6789 0123 4567,  S-1-
5-21-2068569857-8585916410-466756119-23456

   USER,       DOMAIN\USER3,  U3,         3456 7890 1234 5678,  S-1-
5-21-2068569857-8585916410-466756119-34567
];
```

In this example, NTSID has been added, requiring the user accessing the document to be logged into a specific machine in the domain.

Example 5:

```
Section Access;
LOAD * INLINE [
   ACCESS,    USERID,     PASSWORD,   OMIT
   ADMIN,     ADMIN,      ADMIN,
   USER,      USER1,      U1,         SALES
   USER,      USER2,      U2,         WAREHOUSE
   USER,      USER3,      U3,         EMPLOYEES
   USER,      USER4,      U4,         SALES
   USER,      USER4,      U4,         WAREHOUSE
   USER,      USER5,      U5,         *
];

Section Application;
LOAD * INLINE [
   SALES,     WAREHOUSE,  EMPLOYEES,  ORDERS
   1,         2,          3,          4
];
```

In this example, the field OMIT has been added as part of Section Access.
USER1 will not be able to see the field SALES, USER2 will not be able to see field WAREHOUSE and USER3 will not see field EMPLOYEES.

USER4 has been added twice to the solution since we want to OMIT two fields for this user, SALES and WAREHOUSE.

USER5 has a “*” added which means that all listed fields in OMIT will be unavailable.
USER5 will not be able to see fields SALES, WAREHOUSE and EMPLOYEES.

Example 6:

```
Section Access;
LOAD * INLINE [
   ACCESS,    USERID,       PASSWORD,    REGION
   ADMIN,     ADMIN,        ADMIN,
   USER,      USER1,        U1,          AFRICA
   USER,      USER2,        U2,          AMERICA
   USER,      USER3,        U3,          ASIA
   USER,      USER4,        U4,          EUROPE
  USER,       USER5,        U4,          AMERICA
   USER,      USER5,        U5,          *

];

Section Application;
SALES:
LOAD * INLINE [
   REGION,    PROFIT
   AFRICA,    1000
   AMERICA,   2000
   ASIA,      3000
   EUROPE,    4000
   OCEANIA,   5000
];
```

In this example a reduction field has been added called REGION. The purpose is to limit the USERS to their sales region profits.

USER1 will only be able to see the profits for AFRICA, USER2 the profits for AMERICA and USER3 will only see the profits for the ASIA region.

USER4 will be able to see the profits for EUROPE and AMERICA.

USER5 will be able to see all regions listed in the reduction field REGION except for OCEANIA.
Even if USER5 has "*" for the REGION reduction field, star means "all listed values" not all values for the field. Since no USER has OCEANIA listed for the REGION field, USER5 will not have access to the values for OCEANIA.

If we want USER5 to see OCEANIA as well, we need to add an extra line in our section access solution

```
   USER,      USER5,        U5,          OCEANIA
```

Closing comments

Section Access is a great way to protect your data and limit access to your applications. My suggestions for anyone implementing Section Access:

- Backup your applications before implementing Section Access.
- Work in multiple copies so that you can step back if you "lock" yourself out.
- Implement Section Access into the hidden script to increase security.
- If reading your Section Access table from an external source, make sure it's safe.
- Keep it simple and start off small.
- Make sure your solution is manageable, meaning that you have a good overview when adding/deleting users from your solution as your company grows.

Additional documents on this topic with more advanced examples will be written at a later stage.
Please send any comments and/or suggestions to gustav.guldberg@qlikview.com

Gustav Guldberg
QlikTech Inc