Apparo Fast Edit

Setting up security and security based features

Version 3.0.7

1 Basics

Apparo Fast Edit is automatically using the security system of the underlying Business Intelligence system like Qlik Sense or IBM Cognos Analytics.

The only exception is the Standalone version, which supports either MS Active Directory (with SSO) or LDAP.

If you want to enter more than one security group, you need to **separate the groups by comma**.
Example: Group_A, Group_B, Group_C.

You can use placeholders as * and & too:
controlling* is the same like controllingAfrica, controllingEurope

The most security settings are white list based, which means if you enter one or several security groups then the access is restricted to those groups. If you leave it empty, then all users have full access.

Hint: Security group names are case-sensitive

2 Security user types

There are two different user types:

- business users (using Business Cases) and
- designer users (creating Business Cases)

2.1 Designer user security

The security settings for designer users are restricted to the access and edit rights within the Apparo designer.

2.2 Business user security

The security settings for business users are mainly focused on the question:

Who is allowed to see, change or insert data, which means security groups are used to filter data, restrict the access or control features and the behaviour of widgets.

3 Designer user security

3.1 Security hierarchy

The security is hierarchically organized.

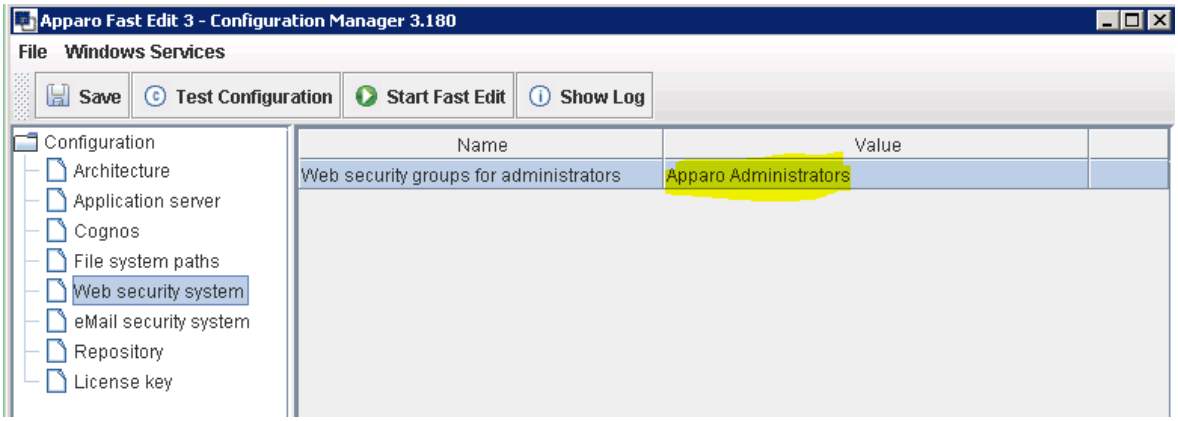
From top to bottom:

- Security settings of the Configuration Manager
- Security settings on client level
- Security settings on folder level
- Security settings on database connection level

3.2 Security settings of the Configuration Manager

The Configuration Manager contains two different properties for security settings.

3.2.1 Web security system



Members of the entered security groups **have full access rights to the Apparo Designer** and can create, alter and delete clients. **They have system wide no limitations**.

These users can run all Business Cases of all clients without limitations.

Hint: If left empty all users accessing the designer have full rights, even in case the following security levels deny this.

3.3 Security on client level

Defines restrictions for accessing secured parts of Apparo Fast Edit designer of a client.

Only members of the listed security groups will be able to access the particular functions.

If no access rights are defined, the access to function is unrestricted for all designer users.

Apparo Client Administrator: Has unrestricted access to all features of this client

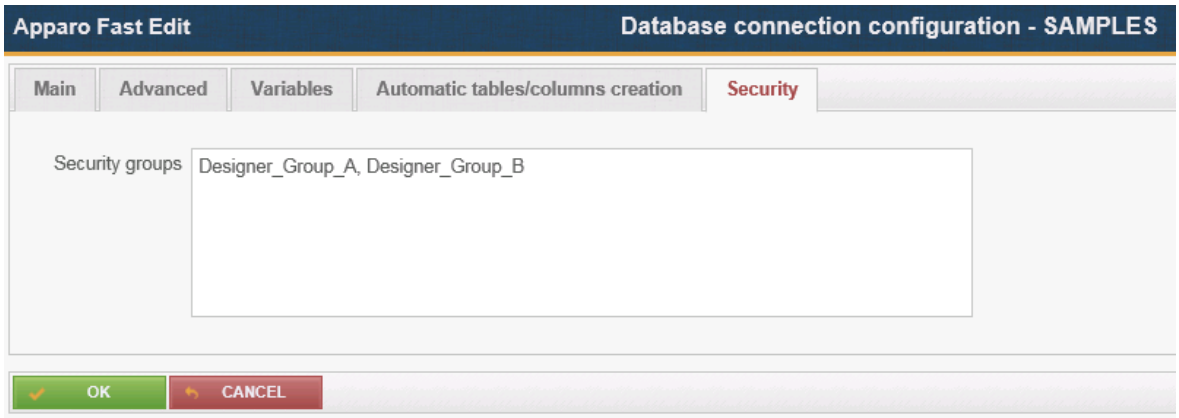
Apparo Connection Administrator: Can create, edit and delete database and email server connections

Apparo Designer: Manages Business Cases - can create, delete and edit Business Cases and folders

Apparo Import & Export Administrator: Can import and export Business Cases and connections

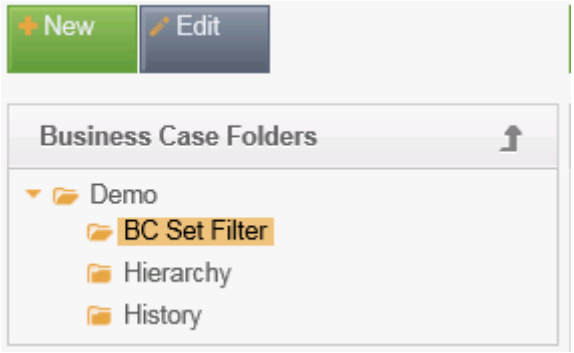
3.4 Security on database connection level

White list of designer users who are allowed to use this database connection.



3.5 Folder security

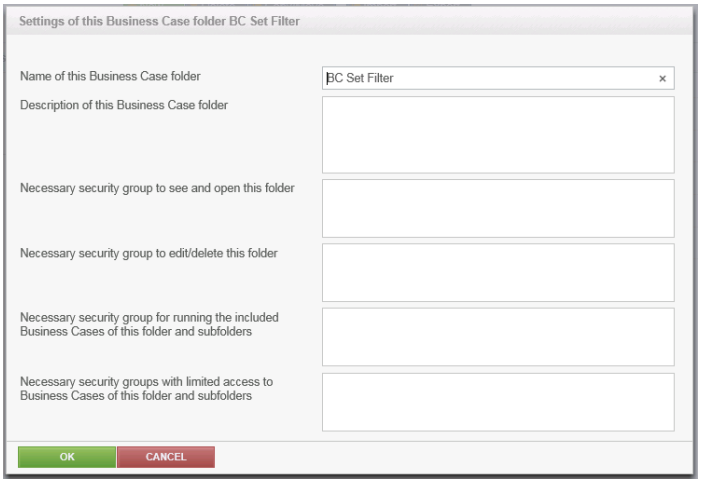
Select the folder and click 'Edit' to open the folder properties:



Depending on the given rights, the user can:

- Create new folders and subfolders
- Delete folder and its contents (subfolders, business cases)
- Change the properties of the folder

Folder properties:



The following security properties are mapped to designer users:

- The necessary security group to see and open this folder
- The necessary security group to edit/delete the folder

4 Business user security

4.1 Security hierarchy

The security is hierarchically organized.

From top to bottom:

- Security setting on Configuration Manager level (= System Administrator)
- Security settings on client level
- Security settings on folder level
- Security settings on Business Case level
- Security settings on feature level
- Security settings on Widget level

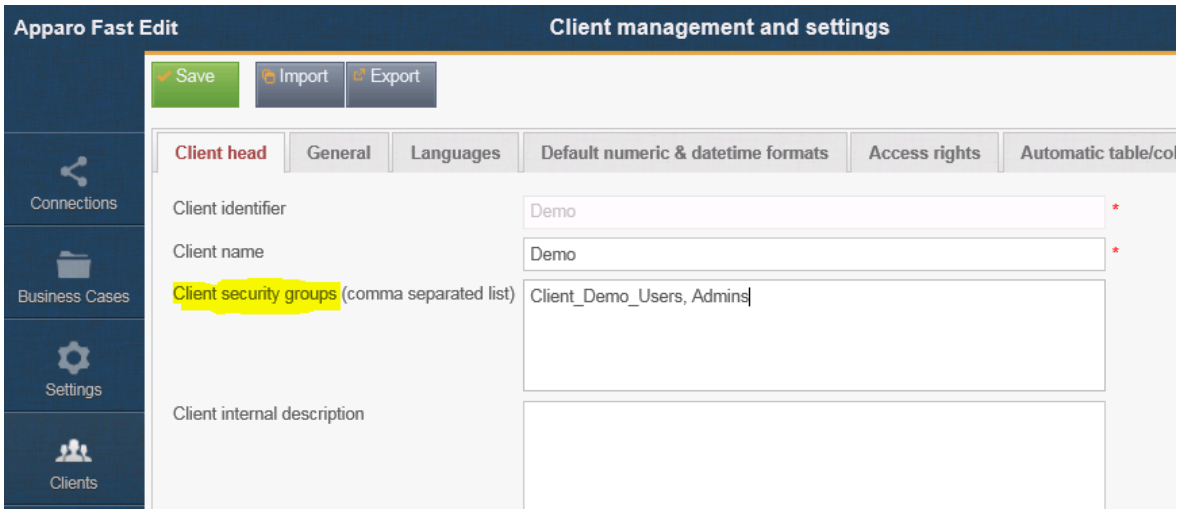
4.2 Security settings on client level

The security groups here are used to assign users and to check the authorization.

Authorization:
Apart from administrators are only users who are member of the entered security groups, entitled to run the Business Cases of this client.

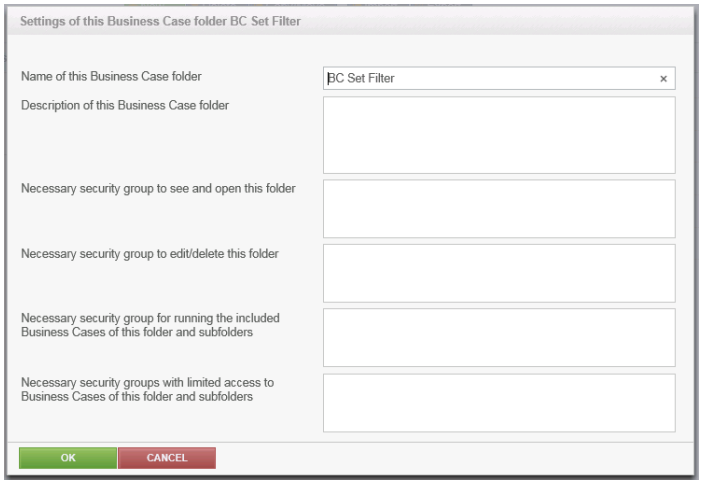
Assignment:
When you open a Business Case without client ID, e.g. from a BI report or an e-mail, the security group of clients will be used to assign the appropriate Business Case.

Without security group or if the user is member of more than on client, the allocation of Business Cases with the same ID, existing in different clients, is based on the order of the clients in the list from top to bottom.



Contains a list of assigned user groups

4.3 Security settings on folder level



The following security properties are mapped to **business users** security settings:

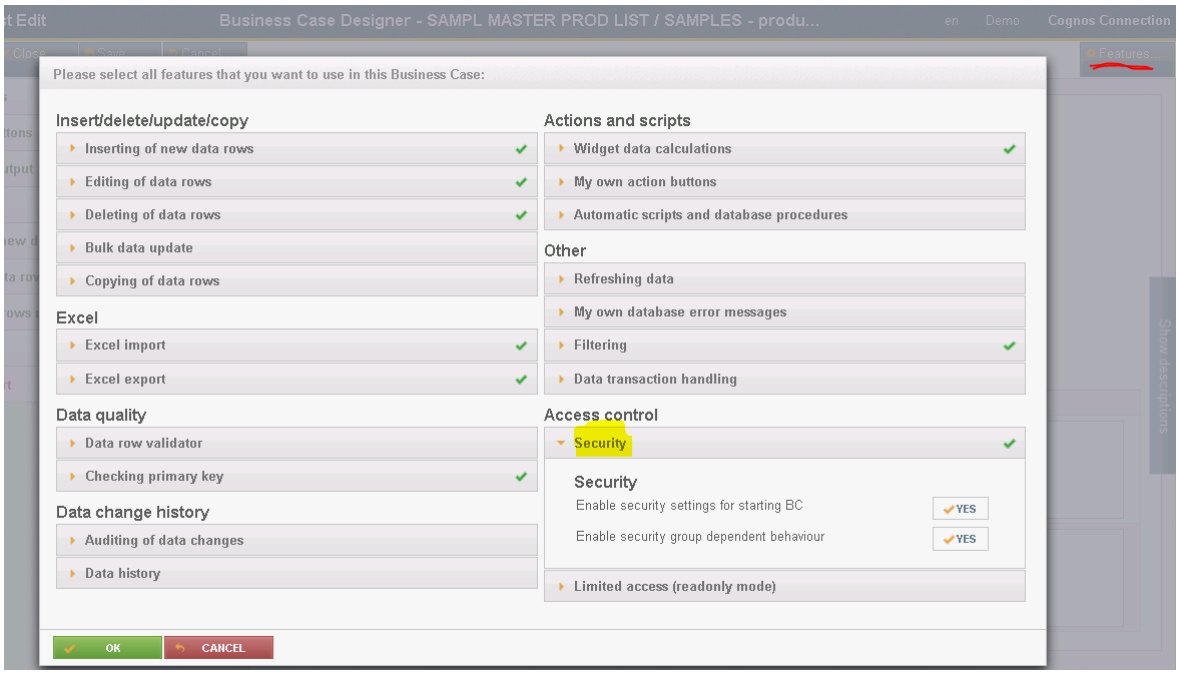
- The necessary security group for running included Business Cases of this folder & subfolders
- The necessary security with limited access to Business Cases of this folder & subfolder

Limited access means, for members of the entered user groups the Business Case starts in Read-only mode. Data changing, entering, import, auto scripts and data changing buttons are disabled.

4.4 Security settings on Business Case level

The security on Business Case level must be enabled first.

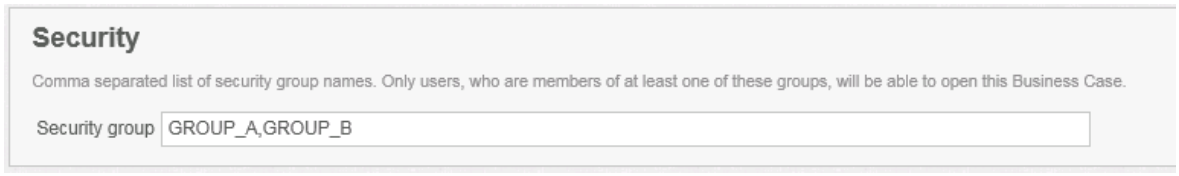
Click the '**Features'** button in the top right corner of the Business Case edit view.
The security settings can be enabled in the chapter 'Access Control' in the tab 'Security'



Enabling security settings for starting BC will add the 'Security' to the left menu, while enabling security group dependent behavior will enable all security settings on widget and feature level.

4.4.1 Menu 'Security'

Allows to enter security groups separated by commas. It limits the general access to the business case (whitelist).



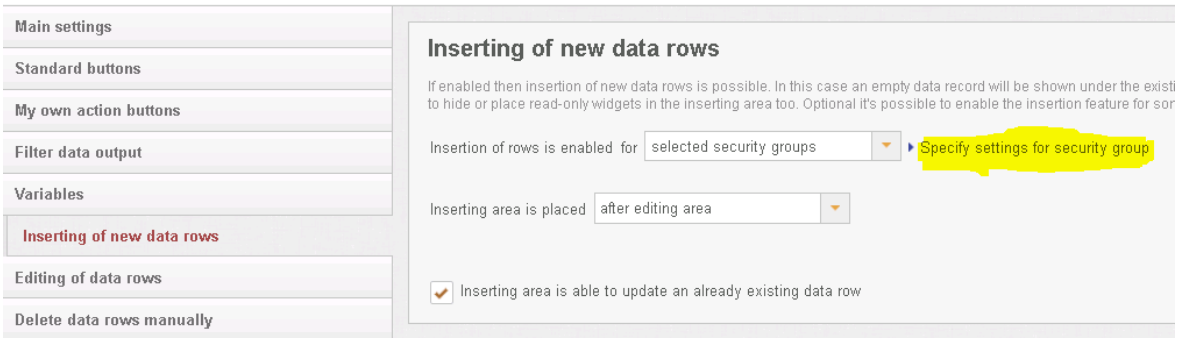
4.5 Security settings on feature level

These settings belog to security group dependent behavior settings and need to be enabled in 'Features' first.

Many features can be enabled for entered security groups only:

- Inserting, Editing, Deleting of data rows
- Excel export
- Automatic scripts and db procedures
- Filter

In the most cases you need to specify the security groups that are allowed to use the feature in a separate window.



When clicking the link the following window appears:

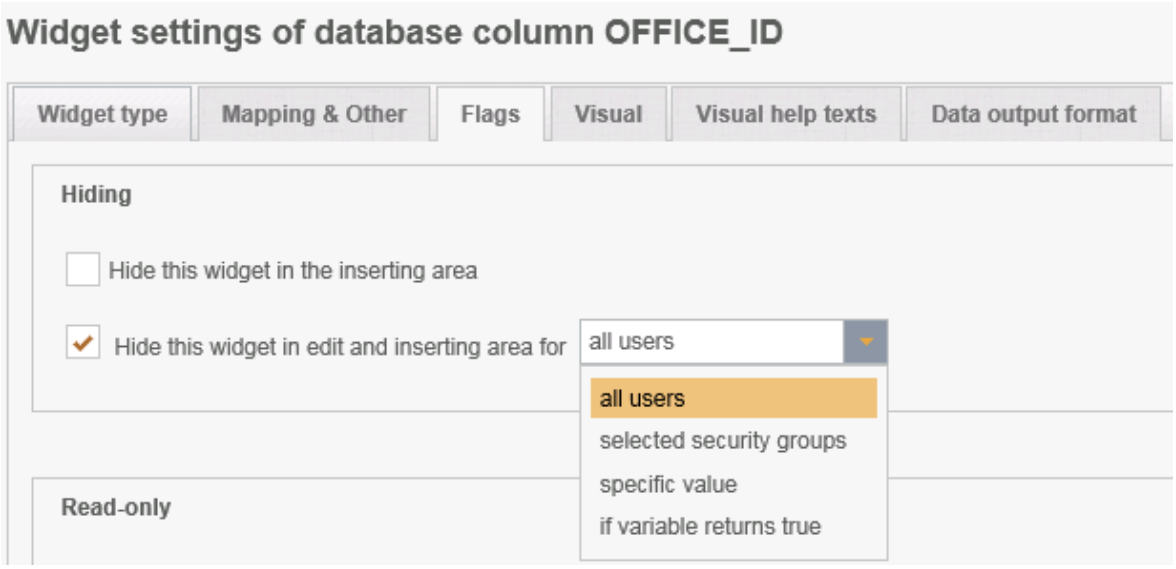
Here you can add the security groups that are allowed to use this feature.

The filter security settings are different and will be explained in the chapter:
Different settings for different security groups

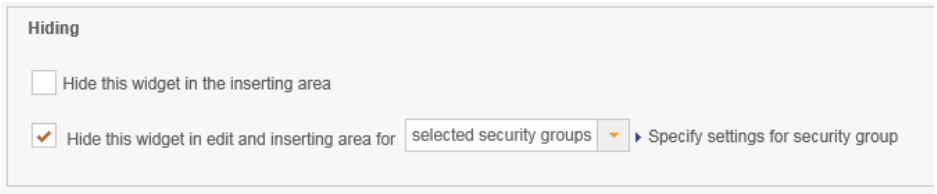
4.6 Security settings on Widget level

Security settings on Widget level are mainly:

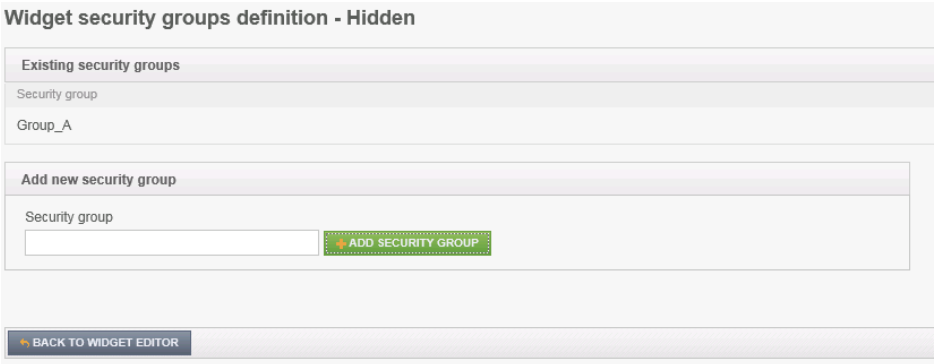
- Settings for hiding or making a Widget read-only
- Default or constant values for different security groups
- Filters on Widget level (when using Lookup or Multiselect Widgets)



Using this setting hides the widget, but only for users who are member of one of the entered user groups. Other users can see the widget.



Hide the widget for the selected user groups



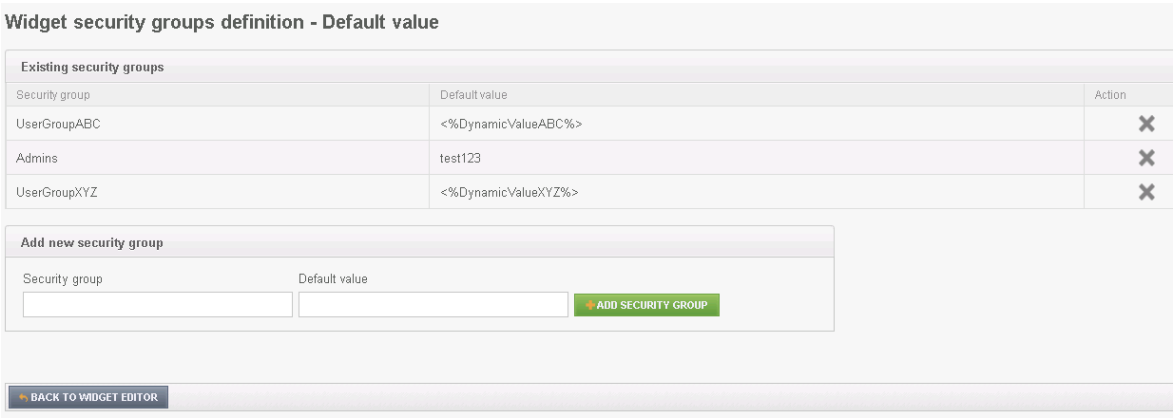
Security group editor

4.7 Different settings for different security groups

Some settings allow to enter different values for different user groups:

- Filters
- Default and constant values

4.7.1 Default and constant values

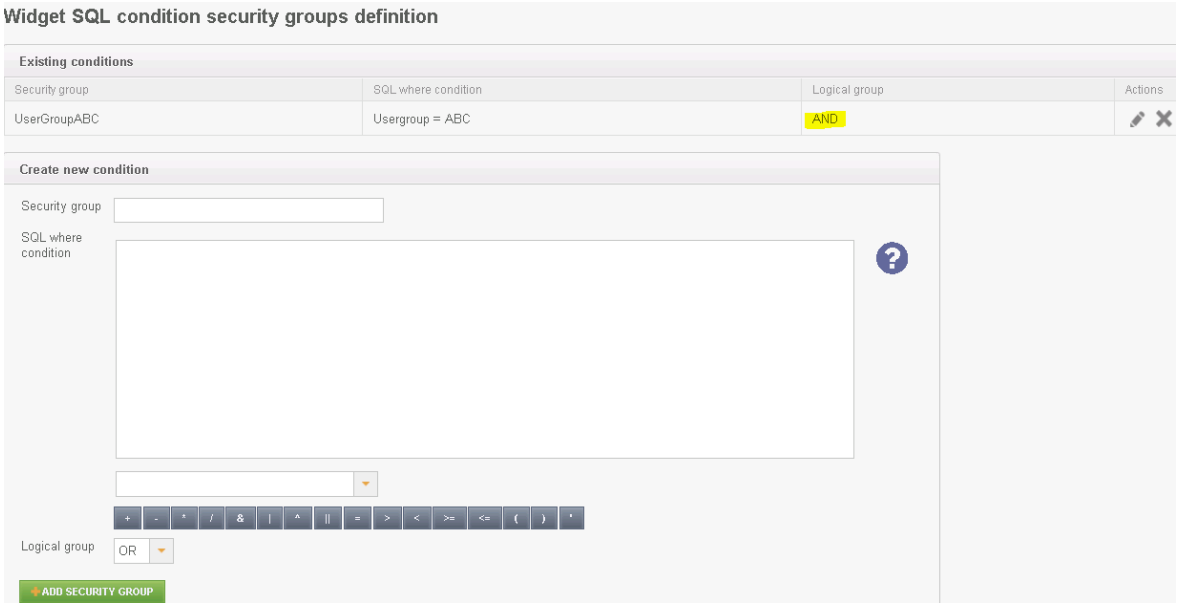


You can enter different value for each used security group, variables are allowed.

4.7.2 Filters

You can enter different filters for each security group.

Entered filters for security groups will not replace but extend the main filter. This can be controlled by the Logical group (AND or OR).



In this example the filter will be ID=<%ID%> AND Usergroup = ABC for the group 'UserGroupABC' and just ID=<%ID%> for all others.

4.8 Retrieving the current users security groups in a variable

For debug and other purposes it can be useful to know all user groups of the current user.
The variable can be output, for example in the header, or further processed for other purposes, e.g. in variables or in filters.

Query the security groups in a Script variable:

```
var groups = afe.getGroupsByRegex('.*');
var result = 'Security groups of the current user: ';
for(var i = 0; i < groups.length; i++) {
  var group = groups[i];
  result = result + group + ', ';
}
// returning the calculated result from script
result;
```

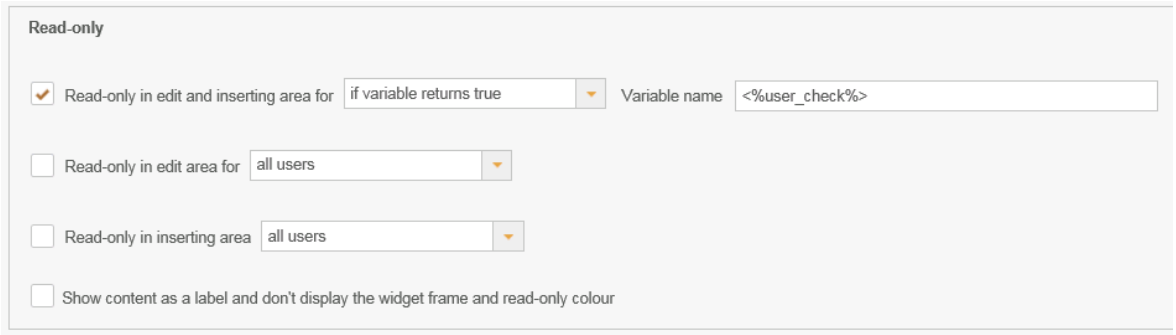
4.9 User based security without groups

To maintain a user based security without groups you will need a user rights table and SQL- & Script variables.

The user rights table contains the user login, the Business Case ID and the rights (read, write, …)

Example:

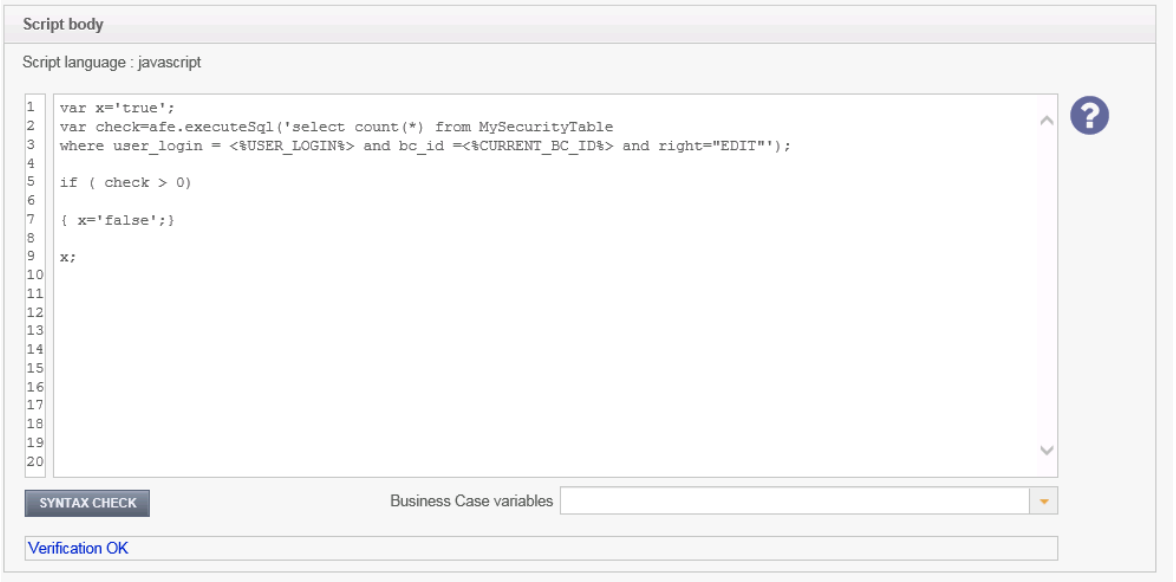
We set a widget to read-only for all users if a variable returns 'true'.



Now we need a script variable that returns always true, except for those who have edit rights.

Script body:

```
var x='true';
var check=afe.executeSql('select count(*) from MySecurityTable
where user_login = <%USER_LOGIN%> and bc_id =<%CURRENT_BC_ID%> and right="EDIT"');
if ( check > 0)
{ x='false';}
x;
```



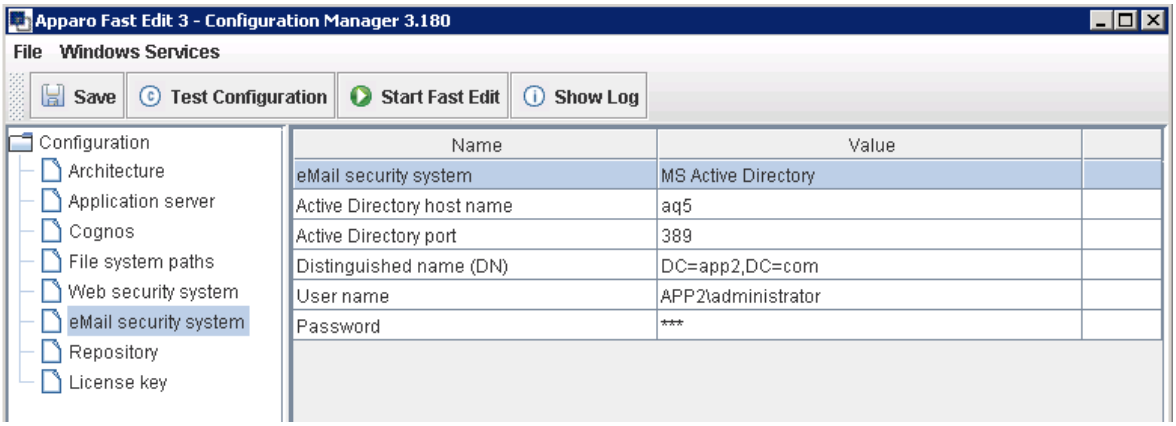
The used SQL statement returns a number > 0 and the used script variable is not longer ‘true’ and becomes editable.

5 E-Mail import security (EIBC)

The import of e-mail attachments is using its own security system and settings.

It can't use the security system of the used Businesss Intelligence system because at this time no user is logged in the BI system.

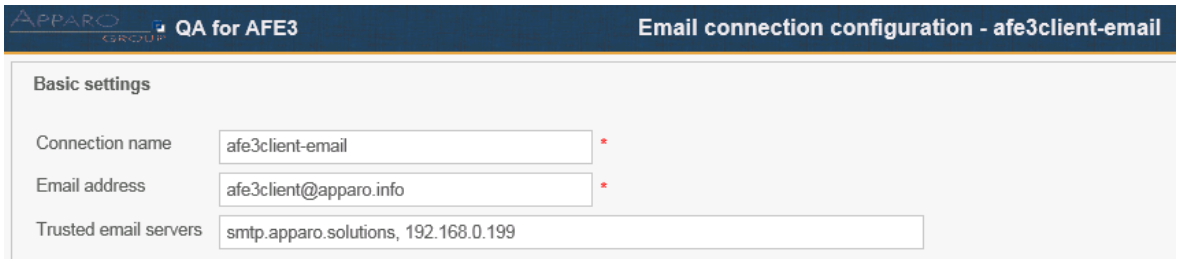
5.1 eMail security system



This only applies when using the feature 'Excel import via E-Mail' (EIBC), this feature is not using the authentication system of the underlying BI system and users do not require a BI user license.

5.2 Security settings of e-mail connections

When setting up the e-mail address that receives the e-mails for the import of attachments, you can enter here a comma separated white list of trusted e-mail servers.

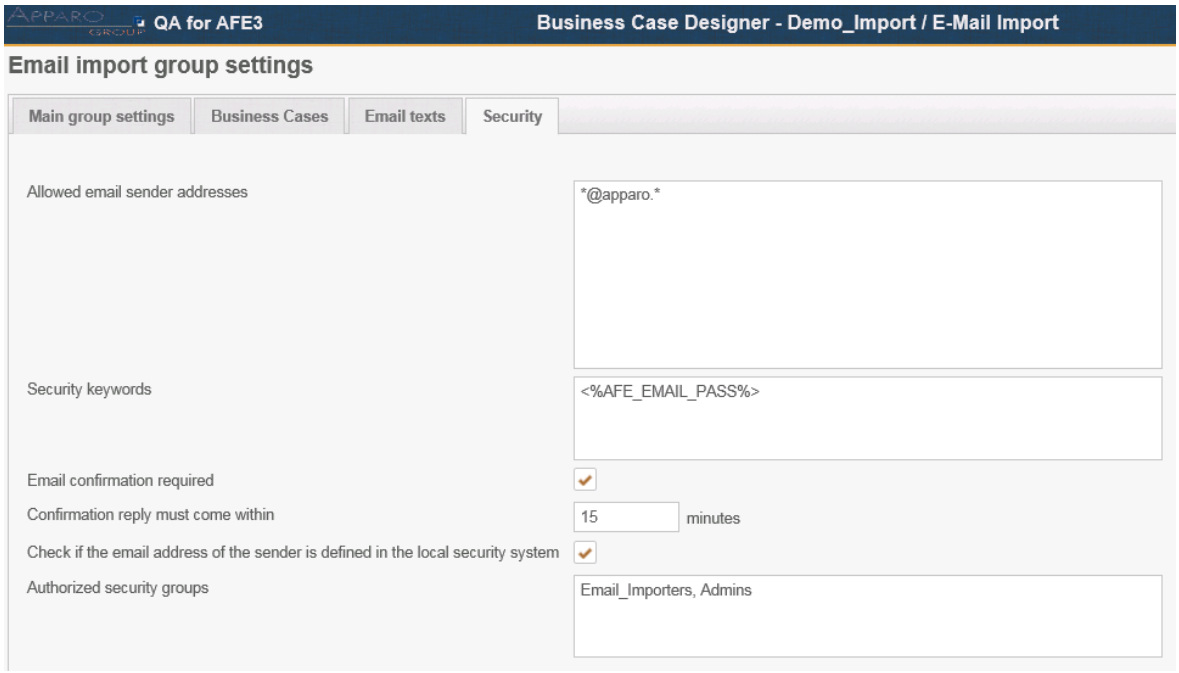


E-Mails received from others sources will be ignored. If left empty, all e-mails are trusted.

5.3 Email import group security settings

E-Mail import Business Cases are containing all settings for the import of email attachments, each can have different email import groups.

Each group contains the settings to import one or several attachements.



Allowed email sender addresses

Comma separated white list of allowed sender addresses. Placeholders (*,?) are allowed.
@apparo. means all senders from apparo.AnyTopLevelDomain is accepted.

Security keywords

A list of comma separated words that every email has to contain in the subject or body. If any of them is missing, the email will be rejected. Leave it empty if you don't want to use this feature.
Variablesare not allowed

Email confirmation required

Sends a confirmation e-mail to the sender of an e-mail to ensure the origin.

Confirmation reply must come within minutes

Timeframe within the confirmation e-mail must be replied, otherwise the import will be rejected.

Check if the email address of the sender is defined in the local security system

Rejects the email if the sender is not defined

Authorized security groups

Contains a list of security groups that are allowed to use this import group