Apparo Fast Edit

Setting up security and security-based features

Version 3.3

1 Basics ... 3
1.1 Security user types ... 4
2 Business user security ... 5
2.1 Security hierarchy ... 5
2.2 Security settings on client level ... 5
2.3 Security settings on designer folder level ... 6
2.4 Enabling security group features on Business Case level ... 7
2.4.1 "Security" feature / Running a Business Case for special security groups only ... 8
2.4.2 "Inserting of new data rows" feature for special user groups only ... 9
2.4.3 "Data output filter" feature depending on security groups ... 10
2.5 Security settings on widget level ... 11
2.5.1 Default and constant values depending on security groups ... 12
2.5.2 Showing widget / readonly widget depending on security groups ... 13
2.6 Retrieving the current user security groups in a variable ... 14
2.7 User based security without groups ... 14
2.8 E-Mail import security (EIBC) ... 16
2.8.1 eMail security system ... 16
2.8.2 Security settings of e-mail connections ... 16
2.8.3 Email import group security settings ... 17
3 Designer user security ... 18
3.1 Security hierarchy ... 18
3.2 Security on client level ... 19
3.3 Security on database connection level ... 20
3.4 Folder security ... 21
4 System administrator user security ... 22

1 Basics

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

For the Apparo Stand-Alone version it is using 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

Please note:

If you use security groups then it is important to restrict Apparo on system level too. Therefore please look into the chapter "System administrator user security" too.

1.1 Security user types

There are 3 different user types:

- **business users** (using Business Cases, the normal user)

  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 output and input, restrict the access or control features and the behaviour of widgets.

- **designer users** (creating Business Cases, the administrator and designer)

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

- **System administrator users**

  Caring about system administration & configuration

2 Business user security

The behaviour of a Business Case can depend on security groups too.

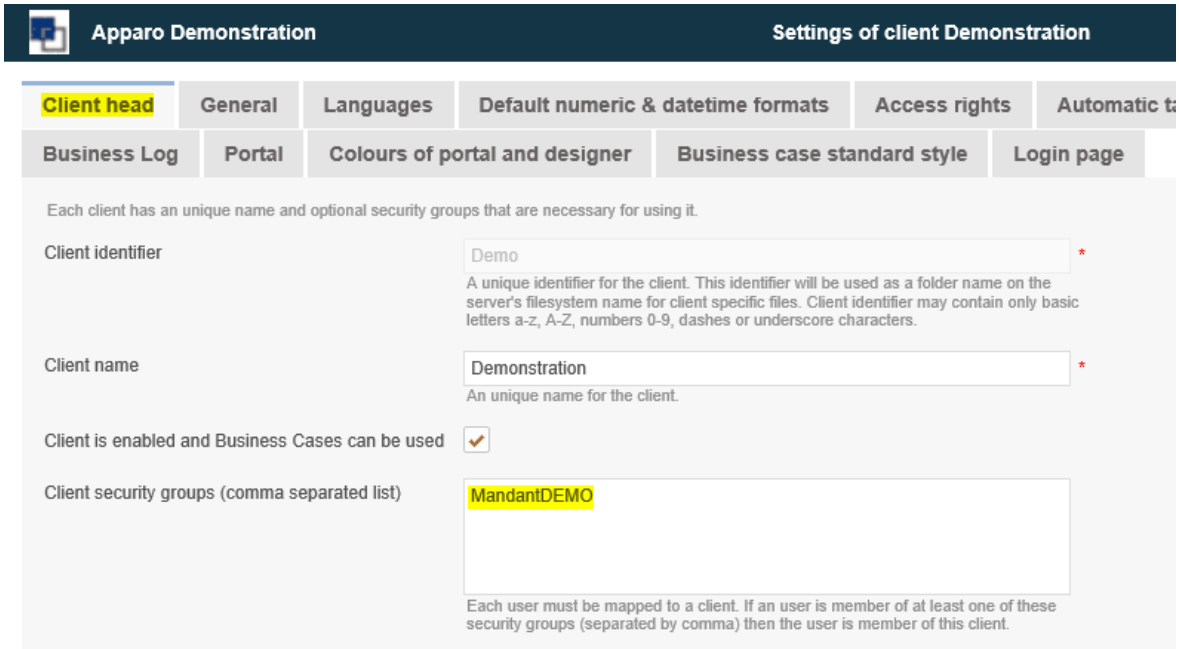
2.1 Security hierarchy

The security is hierarchically organized.

From top to bottom:

- Security settings on **client** level
- Security settings on **designer folder** level
- Security settings on **Business Case** level
- Security settings on **feature** level
- Security settings on **widget** level

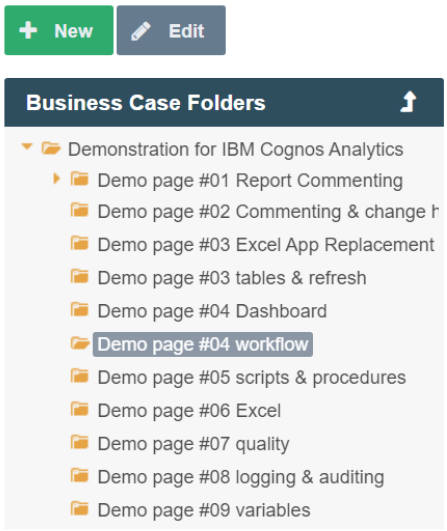
2.2 Security settings on client level



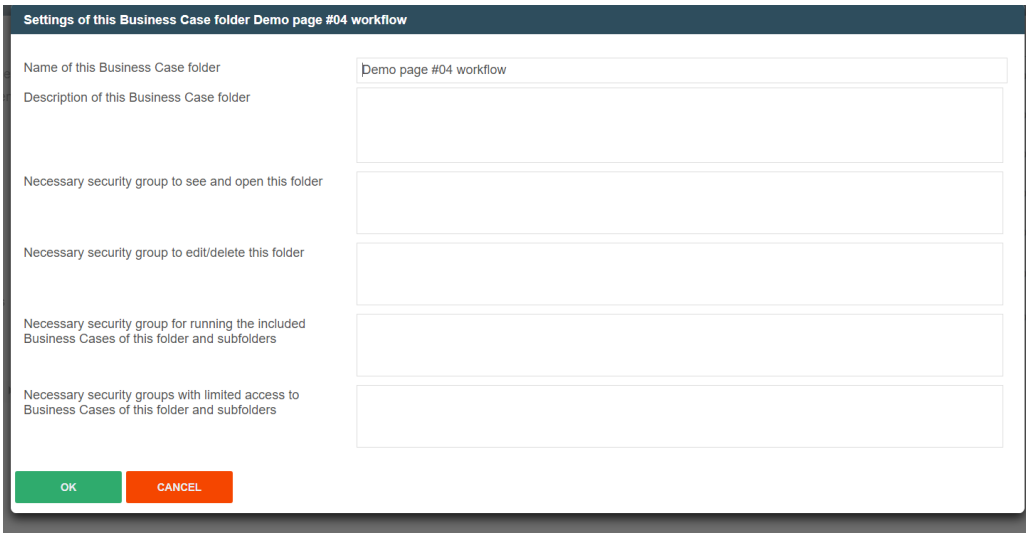
If you add users group(s) here then each business user **must be member of at least 1 group** to be able to **run a Business Case** of this client.

2.3 Security settings on designer folder level

The folders are in the Apparo Designer, left side:



Just press the “Edit” button and you see:



You can use security groups for controlling

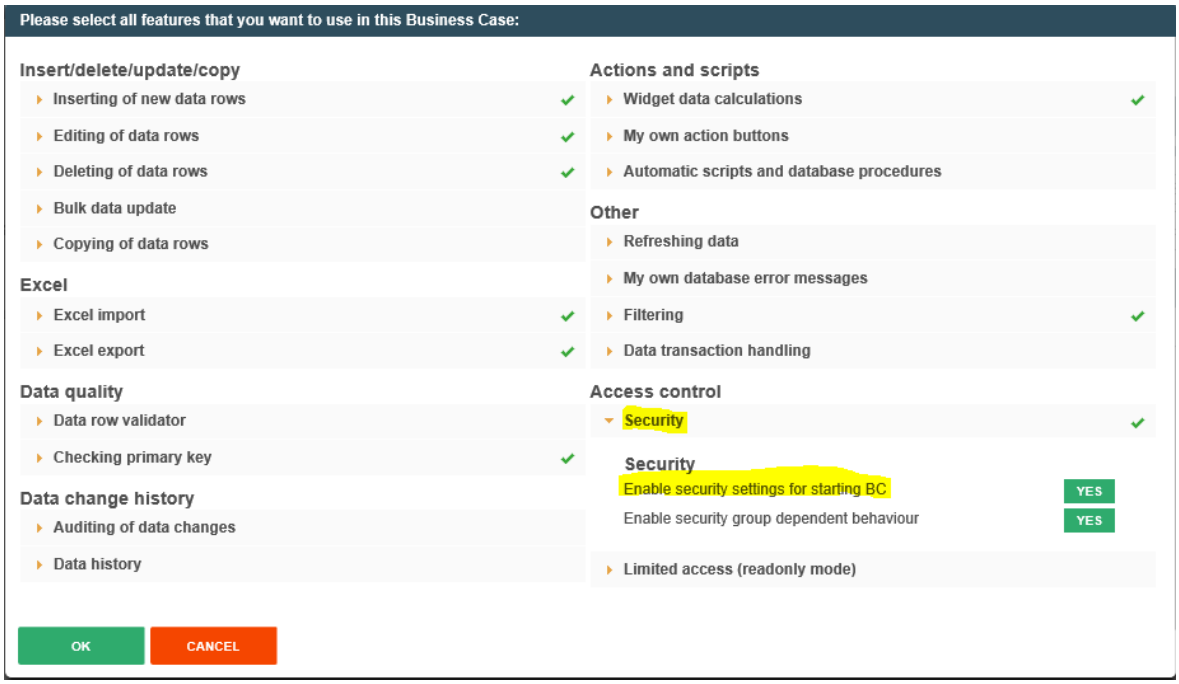
- what user group can **see/open, edit/delete this folder**
- what user group can **run the Business Cases** that are inside a folder
- what user group can **see the Businness Cases in read-only mode** (limited access) only

2.4 Enabling security group features 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.

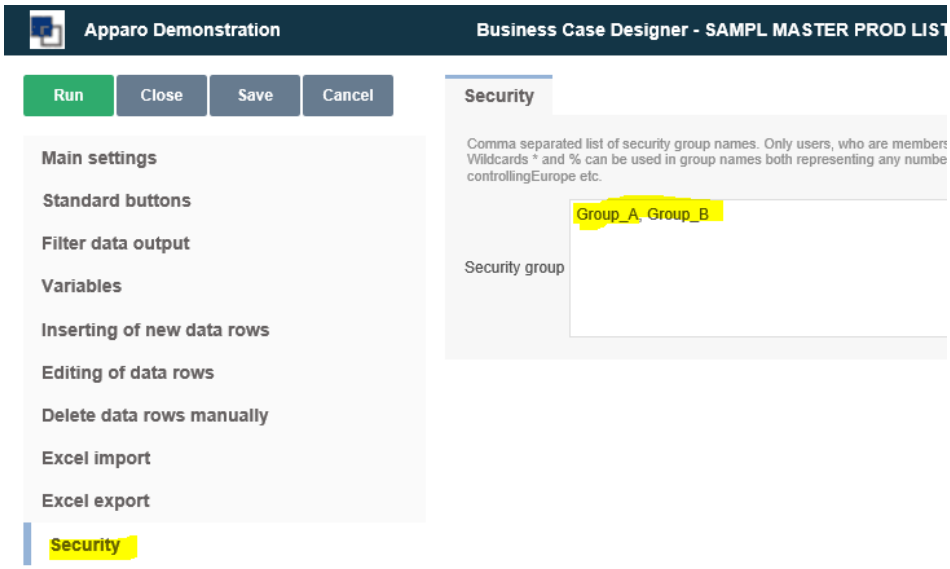
The security features can be enabled in the chapter '**Access control**' in the tab '**Security':**



- **Enabling security settings for starting BC** will add the feature who can run this Business Case
- **Enabling security group dependent behaviour** will enable all security settings on widget and feature level.

2.4.1 “Security” feature / Running a Business Case for special security groups only

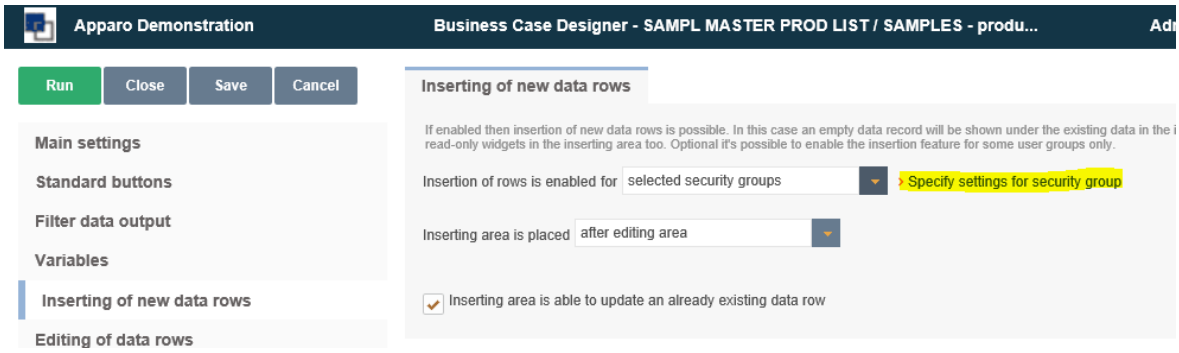
Allows to enter security groups separated by commas. It limits the running of the Business Case (whitelist).



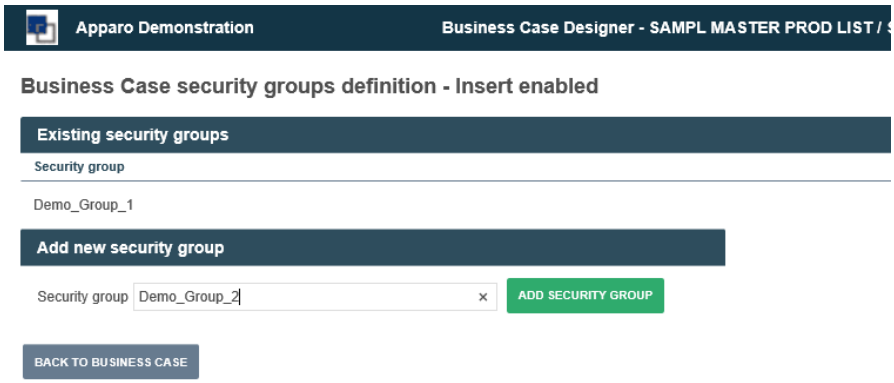
2.4.2 “Inserting of new data rows” feature for special user groups only

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

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



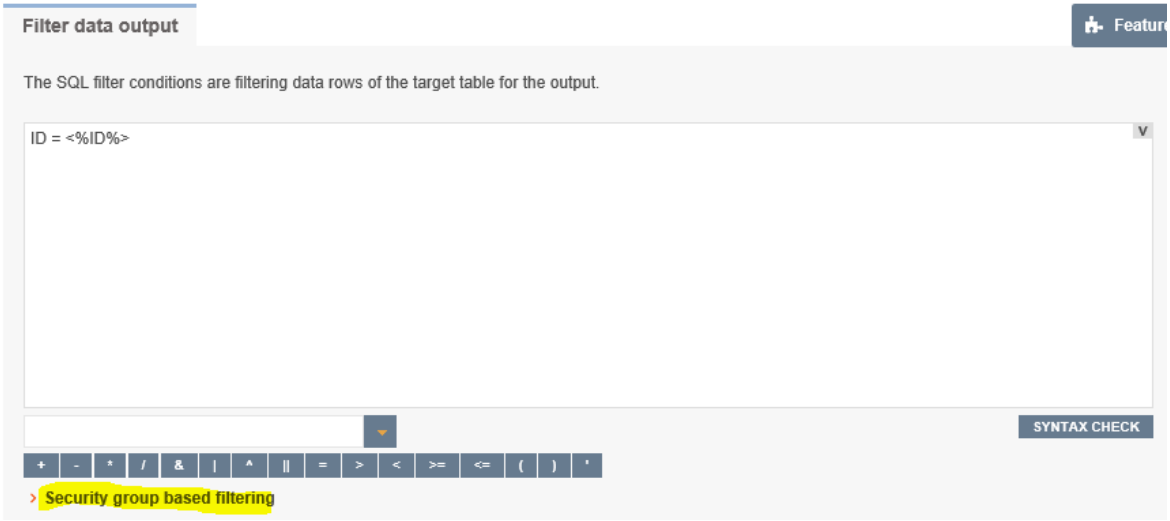
When clicking the yellow marked link the following window appears:



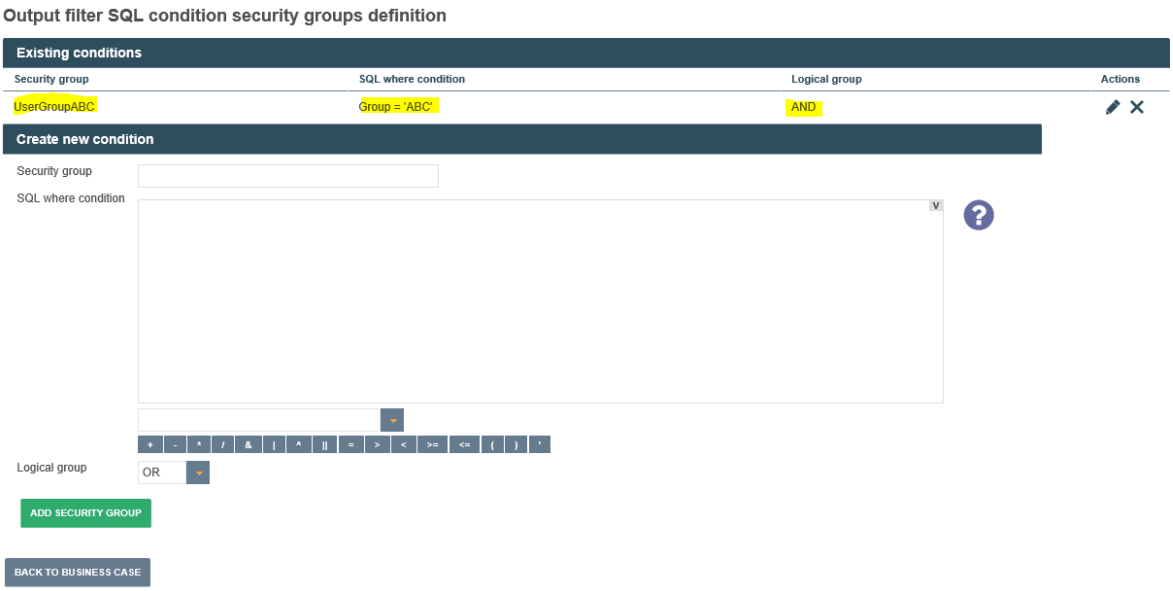
Here you can add the security groups that are allowed to use this feature.

2.4.3 “Data output filter” feature depending on security groups

You can enter different output 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).



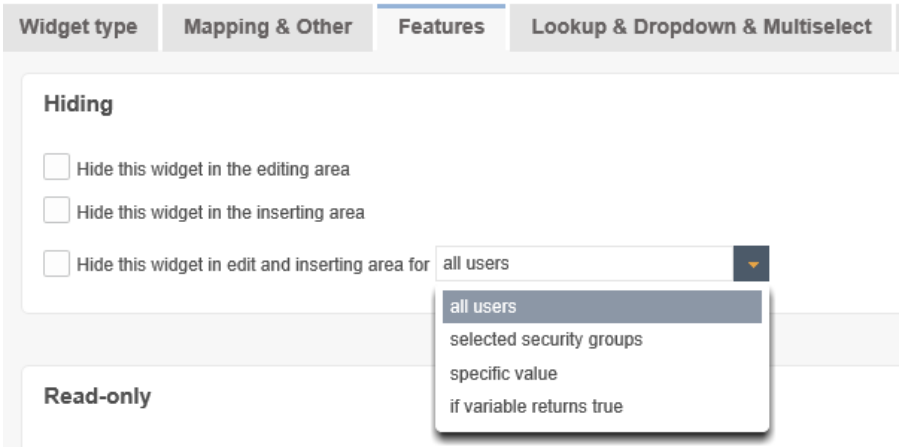
In this example the filter will be

- **ID=<%ID%> AND Group=’ABC’** for the group **UserGroupABC**
- and just **ID=<%ID%>** for all others.

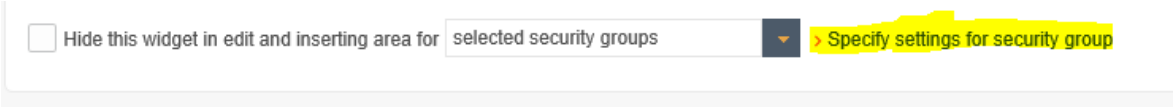
2.5 Security settings on widget level

Security settings on Widget level are mainly:

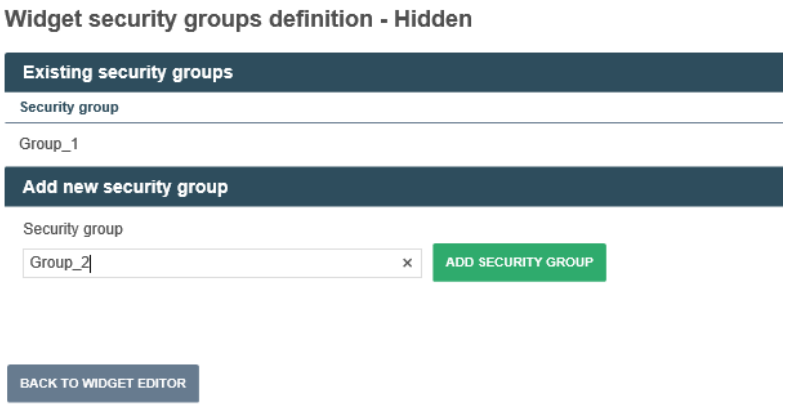
- Settings for hiding or making a Widget read-only
- Default or constant values for different security groups
- Filters on Widget level (when using Lookup or Multiselect Widgets)



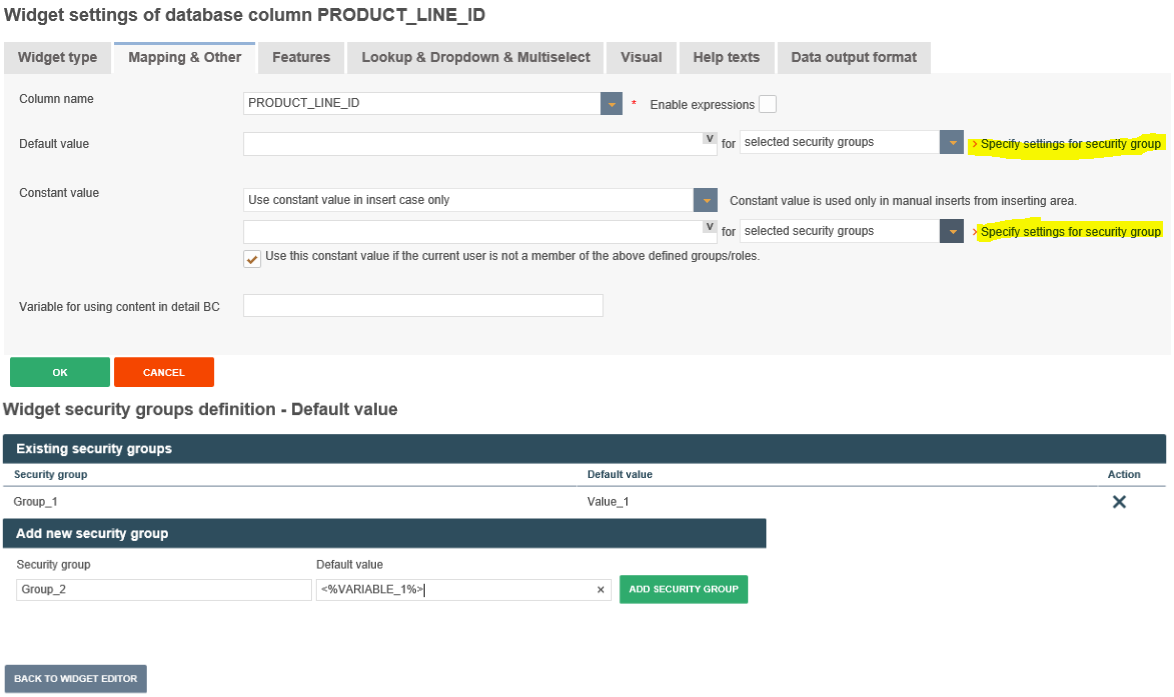
Using this setting hides the widget, but only for users who are member of one of the entered user groups. Other users can see the widget.



Hide the widget for the selected user groups



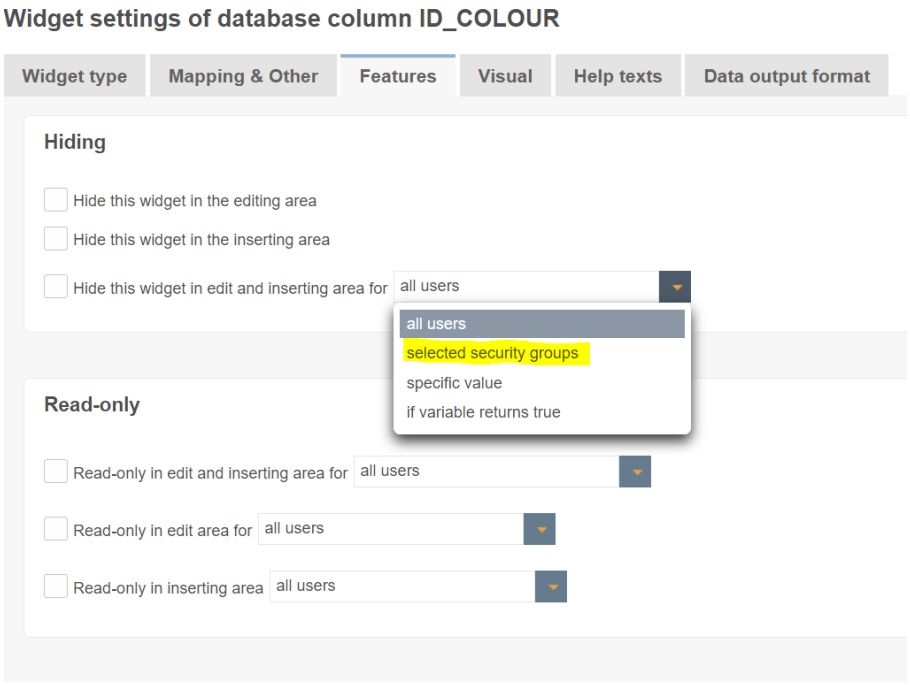
2.5.1 Default and constant values depending on security groups



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

2.5.2 Showing widget / readonly widget depending on security groups

You can control the widget behaviour using the “Features” tab of the widget:



2.6 Retrieving the current user 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 a string with all security groups of the current user
result;
```

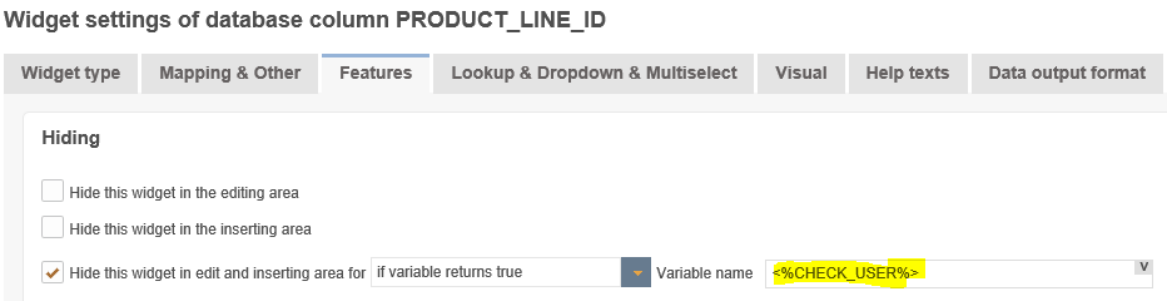
2.7 User based security without groups

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:

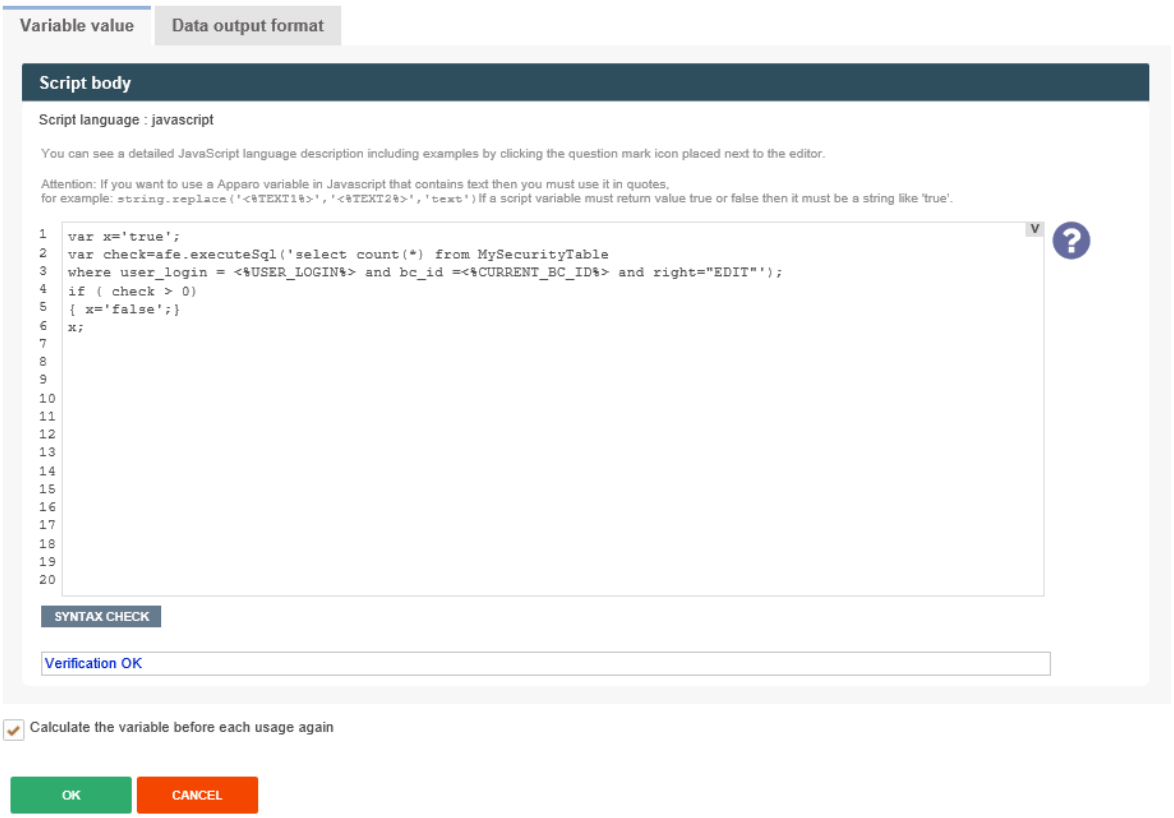
We set a widget to read-only for all users if a variable returns 'true'.



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;
```



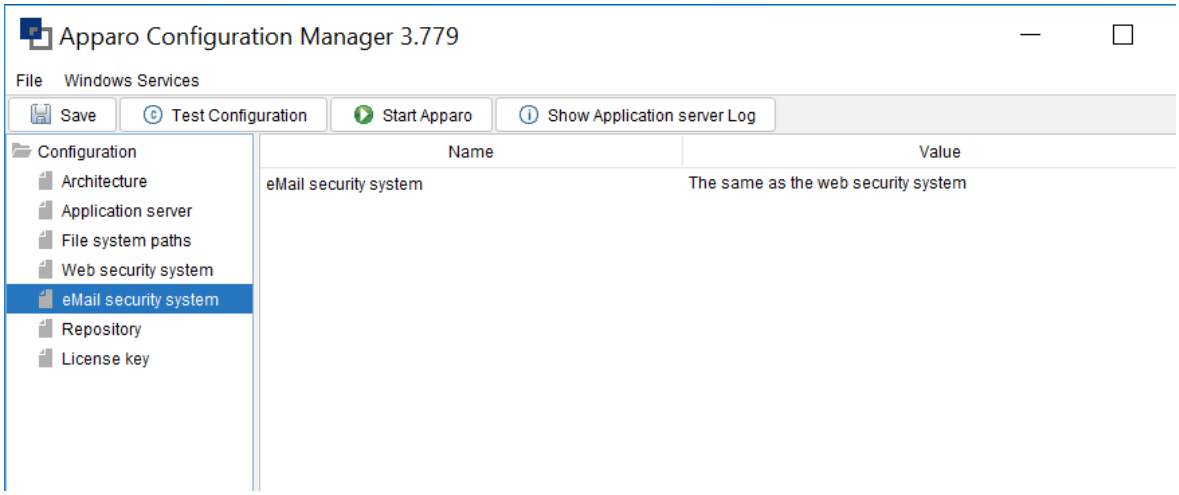
The used SQL statement returns a number > 0 and the used script variable is not longer ‘true’ and becomes editable.

2.8 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.

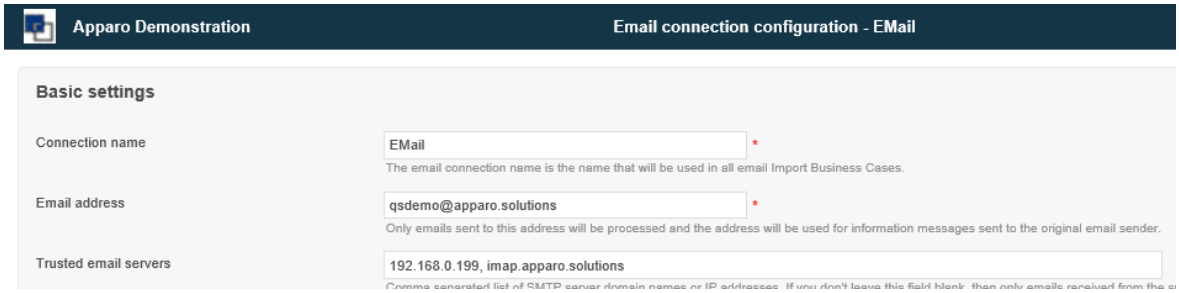
2.8.1 eMail security system



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.

2.8.2 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.

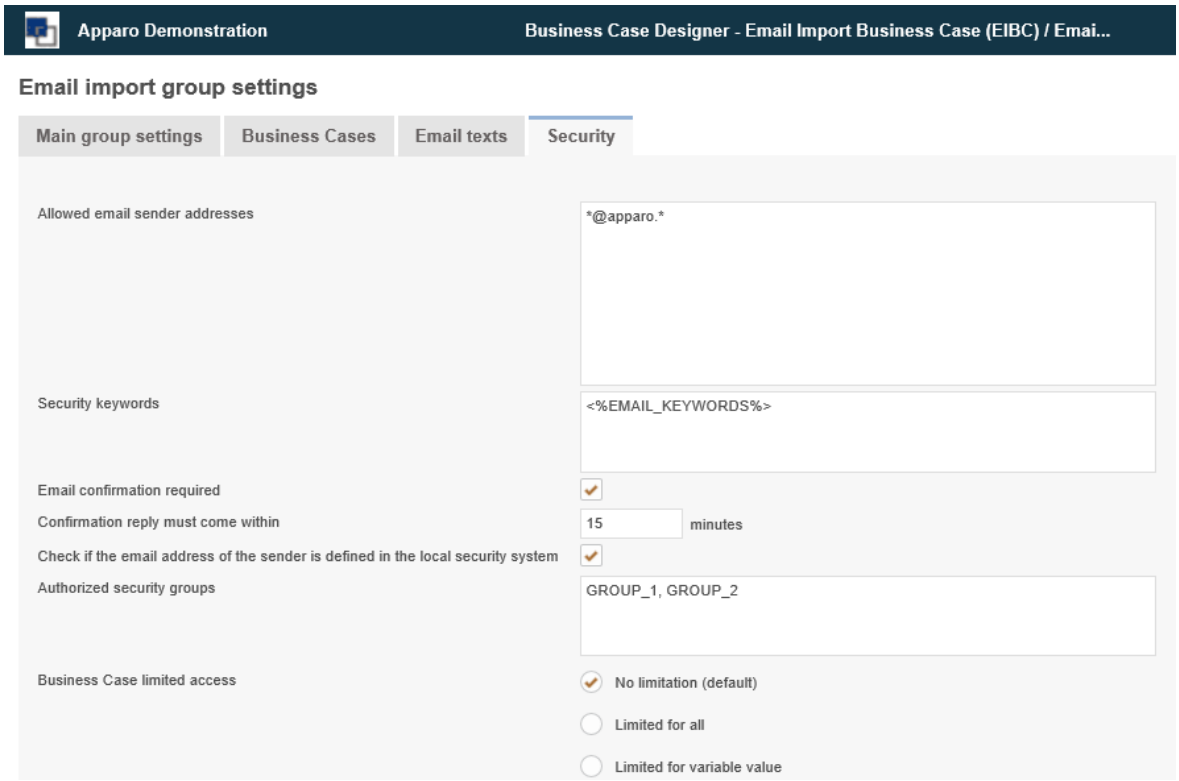


E-Mails received from others sources will be ignored. If left empty, all e-mails are trusted.

2.8.3 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.
Variables are 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

3 Designer user security

It is possible to restrict the access/usage in the Apparo Designer.

3.1 Security hierarchy

The security is hierarchically organized.

From top to bottom:

- Security settings on **client** level
- Security settings on **folder** level
- Security settings on **database connection** level

3.2 Security on client level

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

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

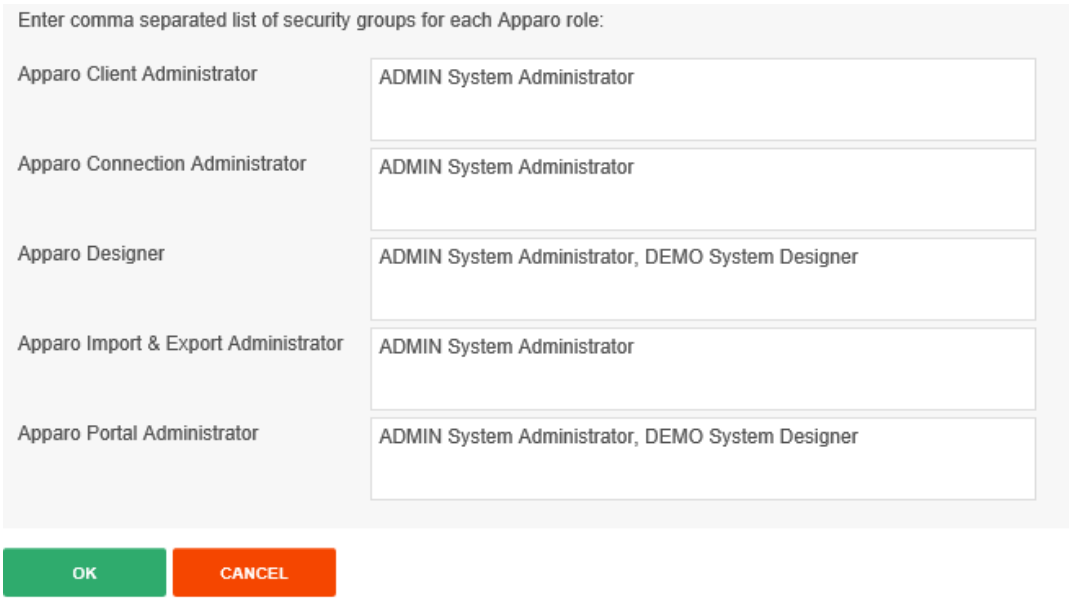
If no access rights are defined, the access to function is unrestricted for all designer users.

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

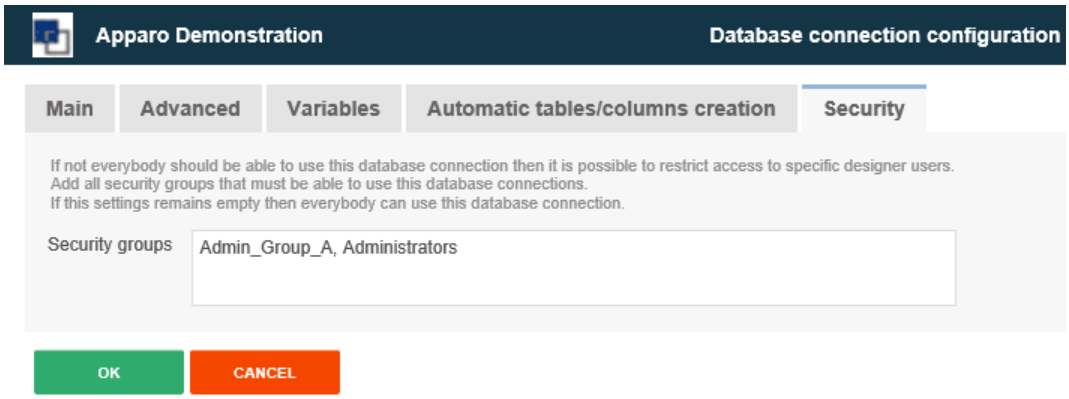
Apparo Import & Export Administrator: Can import and export Business Cases and connections



Hint: Apparo Portal Administrator is available in Stand-alone version only

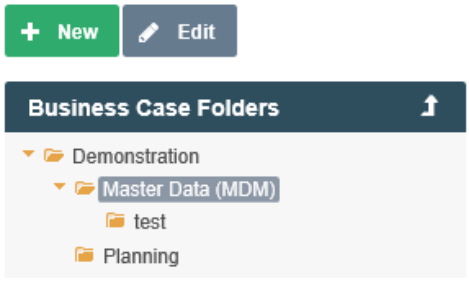
3.3 Security on database connection level

You can define what group of designers can use a database connection or not.



3.4 Folder security

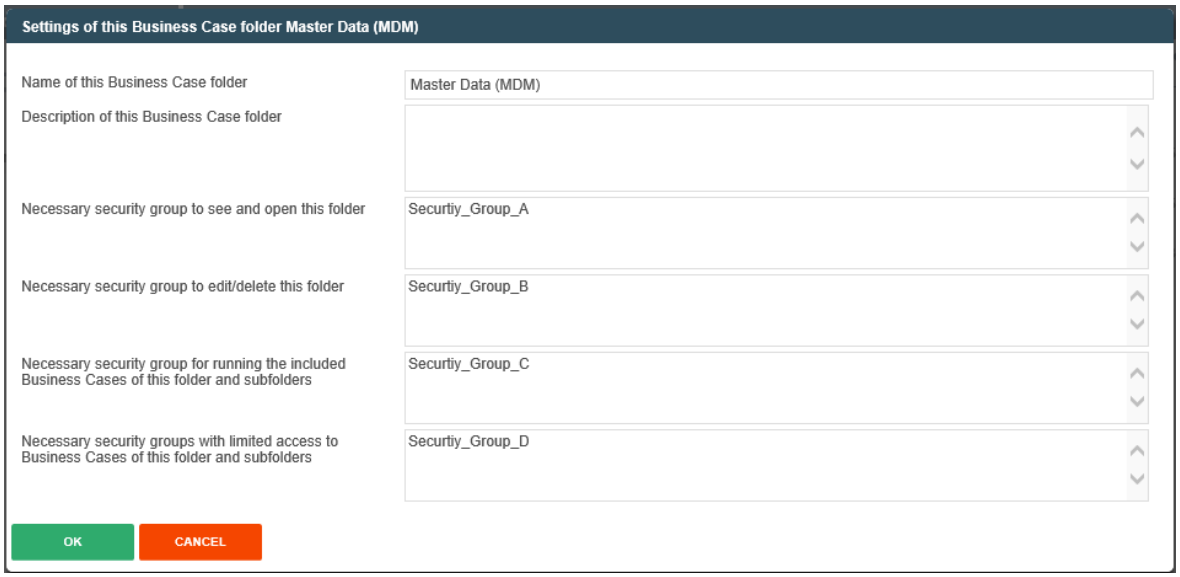
Select the folder and click 'Edit' to open the folder properties:



Depending on the given rights, the user can:

- **See and open** folders and subfolders
- **Edit and delete** folder and its contents (subfolders, business cases)
- **Running Business Cases** or not of this folder
- **Making Business Cases read-only** for this folder

Folder properties:

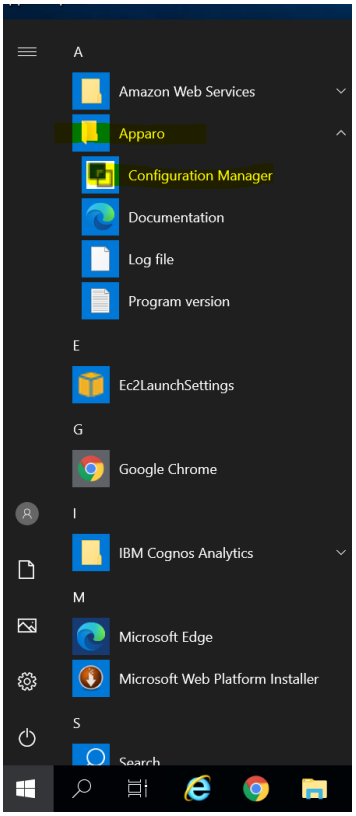


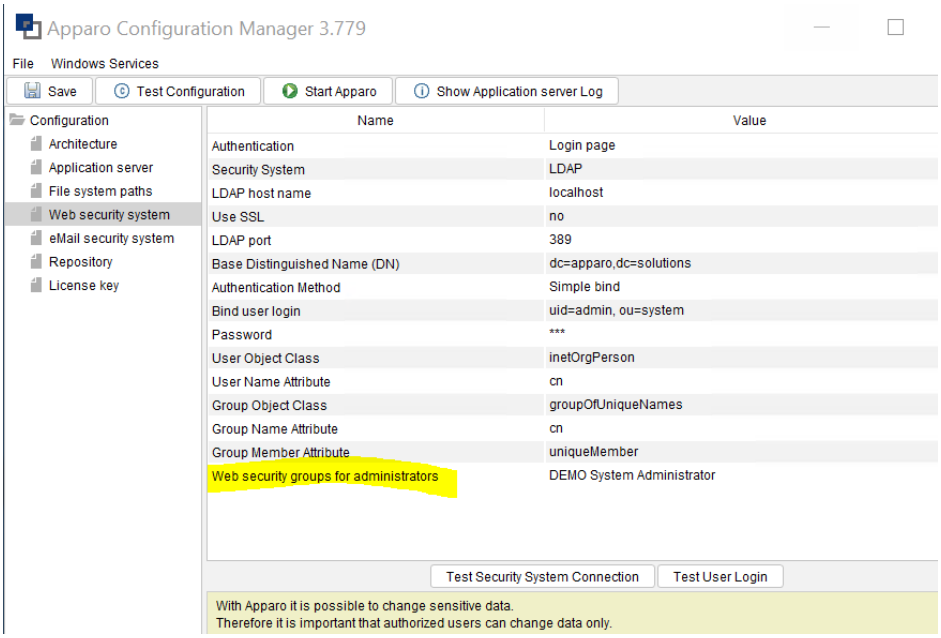
4 System administrator user security

The **Apparo Configuration Manager** contains an important security setting that is defining the name of the security group for **System Administrators**.

You can open it using the Windows Start

… or jumping into
[APPARO HOME]\FastEdit\cm
and starting cm.bat or cm.sh





Members of the entered security groups **have full access rights to the complete Apparo system, including 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.

Therefore better making a security group like for example "**Apparo Administrators**" and adding all system users into it.

After you have added this name into "**Web security groups for administrators**" please press "**Start Apparo**".