

Apparo Fast Edit

Setting up security and security-based features

Version 3.3





1	Basic	s	3
	1.1	Security user types	4
2	Busin	ess 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 2.4.1 2.4.2 2.4.3	Enabling security group features on Business Case level "Security" feature / Running a Business Case for special security groups only "Inserting of new data rows" feature for special user groups only "Data output filter" feature depending on security groups	8 9
	2.5 2.5.1 2.5.2	Security settings on widget level Default and constant values depending on security groups Showing widget / readonly widget depending on security groups	12
	2.6	Retrieving the current user security groups in a variable	14
	2.6 2.7	Retrieving the current user security groups in a variable User based security without groups	
			14 16 16 16
3	2.7 2.8 2.8.1 2.8.2 2.8.3	User based security without groups E-Mail import security (EIBC) eMail security system Security settings of e-mail connections	 14 16 16 16 17
3	2.7 2.8 2.8.1 2.8.2 2.8.3	User based security without groups E-Mail import security (EIBC) eMail security system Security settings of e-mail connections Email import group security settings	14 16 16 16 17 18
3	2.7 2.8 2.8.1 2.8.2 2.8.3 Desig	User based security without groups E-Mail import security (EIBC) eMail security system Security settings of e-mail connections Email import group security settings imer user security	14 16 16 17 17 18
3	2.7 2.8 2.8.1 2.8.2 2.8.3 Desig 3.1	User based security without groups. E-Mail import security (EIBC). eMail security system. Security settings of e-mail connections. Email import group security settings. Iner user security Security hierarchy.	14 16 16 17 17 18 18 19
3	2.7 2.8 2.8.1 2.8.2 2.8.3 Desig 3.1 3.2	User based security without groups. E-Mail import security (EIBC). eMail security system. Security settings of e-mail connections. Email import group security settings. Iner user security	14 16 16 17 18 18 19 20



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 <u>restrict Apparo on system level too</u>. 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

🔁 Apparo D	emonstratio	'n		Settings	of client Demo	nstration
Client head	General	Languages	Default numeric &	datetime formats	Access right	s Automatic ta
Business Log	Portal	Colours of po	ortal and designer	Business case st	andard style	Login page
Each client has an	unique name an	d optional security gro	ups that are necessary for us	sing it.		
Client identifier			Demo			*
		A unique identifier for the or server's filesystem name for letters a-z, A-Z, numbers 0				
Client name			Demonstration			*
			An unique name for the clie	ent.		
Client is enabled	and Business (Cases can be used	✓			
Client security gro	oups (comma s	eparated list)	MandantDEMO			
				d to a client. If an user is me I by comma) then the user is		

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:

+ New	🖋 Edit				
Busines	s Case Fol	ders 🧾			
🔻 🗁 Demo	onstration for	IBM Cognos Analytics			
) 📔 De	emo page #0	1 Report Commenting			
i De	emo page #0	2 Commenting & change h			
🧰 De	emo page #0	3 Excel App Replacement			
🧰 De	emo page #0	3 tables & refresh			
🧰 De	emo page #0	4 Dashboard			
🥟 De	emo page #0	4 workflow			
🧰 De	emo page #0	5 scripts & procedures			
i De	emo page #0	6 Excel			
🧎 De	emo page #0 [·]	7 quality			
🧎 De	emo page #0	8 logging & auditing			
🦲 De	emo page #0	9 variables			

Just press the "Edit" button and you see:

Settings of this Business Case folder Demo page #04 workflow				
Name of this Business Case folder	Demo page #04 workflow			
Description of this Business Case folder				
Necessary security group to see and open this folder				
Necessary security group to edit/delete this folder				
Necessary security group for running the included				
Business Cases of this folder and subfolders				
Necessary security groups with limited access to Business Cases of this folder and subfolders				
Business Cases of this folder and subfolders				
OK CANCEL				

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':

Please select all features that you want to use in this Business Case:				
Insert/delete/update/copy		Actions and scripts		
Inserting of new data rows	~	 Widget data calculations 	× .	
 Editing of data rows 	~	My own action buttons		
 Deleting of data rows 		 Automatic scripts and database procedures 		
 Bulk data update 		Other		
 Copying of data rows 		 Refreshing data 		
Excel		 My own database error messages 		
Excel import	~	 Filtering 	~	
Excel export	~	Data transaction handling		
Data quality		Access control		
Data row validator		- Security	× .	
Checking primary key		Security		
Data change history		Enable security settings for starting BC	s	
 Auditing of data changes 		Enable security group dependent behaviour YE	S	
Data history		Limited access (readonly mode)		
OK CANCEL				
 Deleting of data rows Bulk data update Copying of data rows Excel Excel import Excel export Data quality Data row validator Checking primary key Data change history Auditing of data changes Data history 	* *	 Automatic scripts and database procedures Other Refreshing data My own database error messages Filtering Data transaction handling Access control Security Enable security group dependent behaviour Yet 	 ✓ 	

- 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).

Apparo Demonstration	Business Case Designer - SAMPL MASTER PROD LIST
Run Close Save Cancel	Security
Main settings Standard buttons Filter data output Variables Inserting of new data rows	Comma separated list of security group names. Only users, who are members Wildcards * and % can be used in group names both representing any number controllingEurope etc. Group_A_Group_B_ Security group
Editing of data rows	
Delete data rows manually	
Excel import	
Excel export	
Security	



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.

Apparo Demonstration	Business Case Designer - SAMPL MASTER PROD LIST / SAMPLES - produ Adu
Run Close Save Cancel	Inserting of new data rows
Main settings	If enabled then insertion of new data rows is possible. In this case an empty data record will be shown under the existing data in the read-only widgets in the inserting area too. Optional it's possible to enable the insertion feature for some user groups only.
Standard buttons	Insertion of rows is enabled for selected security groups
Filter data output	Inserting area is placed after editing area
Variables	
Inserting of new data rows	Inserting area is able to update an already existing data row
Editing of data rows	

When clicking the yellow marked link the following window appears:

Apparo Demonstration	Business Case Designer - SAMPL MASTER PROD LIST / s
Business Case security groups definitio	n - Insert enabled
Existing security groups	
Security group	
Demo_Group_1	
Add new security group	
Security group Demo_Group_2	X ADD SECURITY GROUP
BACK TO BUSINESS CASE	

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.

Filter data output	📩 Featur
The SQL filter conditions are filtering data rows of the target table for the output.	
ID = <%ID%>	V
S S	YNTAX CHECK
+ - * / & * = > < >= <= () * > Security group based filtering	

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

Existing conditions			
Security group	SQL where condition	Logical group	Actions
UserGroupABC	Group = 'ABC'	AND	ø ×
Create new condition			
Security group			
SQL where condition		×	3
Logical group OR S	► > < >= < < () '		
ADD SECURITY GROUP			
BACK TO BUSINESS CASE			

Output filter SQL condition security groups definition

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)

Widget type	Mapping & Other	Features	Lookup & Dropdown & Multiselect
Hiding			
	vidget in the editing area		
Hide this w	vidget in edit and inserting a	rea for all users	
		selecter	d security groups
Read-only		specific if variab	value ole returns true

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

Widget security groups definition - Hidden

Existing security groups	
Security group	
Group_1	
Add new security group	
Security group	
Group_2	ADD SECURITY GROUP
Group_2	

BACK TO WIDGET EDITOR



2.5.1 Default and constant values depending on security groups

Widget settings of database column PRODUCT_LINE_ID

Widget type	Mapping & Other	Features	Lookup & Dropdown & Multiselect	Visual	Help texts	Data output format	
Column name		PRODUCT_LINE_	ID	 Enab 	le expressions		
Default value					v for select	ted security groups	Specify settings for security group
Constant value			e in insert case only				
		Use constant value	a in insent case only			t value is used only in manua ted security groups	 Inserts from inserting area. Specify settings for security group.
		 Use this consta 	nt value if the current user is not a member of th	e above define			
Variable for using	content in detail BC						
2							
ок	CANCEL						
Widget securi	ity groups definit	tion - Default	value				
Existing securi	ty groups						
Security group			De	fault value			Action
Group_1			Va	lue_1			×
Add new securi	ity group						
Security group		Defaul	It value				
Group_2		<%V/	ARIABLE_1%>	ADD SECU	RITY GROUP		

BACK TO WIDGET EDITOR

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:

Widget settings of database column ID_COLOUR

Widget type	Mapping & Other	Features	Visual	Help texts	Data output format
	vidget in the editing area				
Hide this w	vidget in edit and inserting a	all user selecte specific	s d security gro		
Read-only	in edit and inserting area for in edit area for all users			•	,
Read-only	in inserting area all users				



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;</pre>
```

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'.

Widget settings of database column PRODUCT_LINE_ID

Widget type	Mapping & Other	Features	Lookup & Dropdov	vn & Multiselect	Visual	Help texts	Data output format
Hiding							
Hide this v	vidget in the editing area						
Hide this v	vidget in the inserting area						
✓ Hide this v	vidget in edit and inserting a	rea for if variabl	le returns true	 Variable name 	<%CHECK	_USER%>	V

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;
```



Script language :	javascript	
You can see a det	ailed JavaScript language description including examples by clicking the question mark icon placed next to the editor.	
Attention: If you we	ant to use a Apparo variable in Javascript that contains text then you must use it in quotes,	
	an to use a spear vanade vanade in varazen je nak onnaan tex men jou noar use k in quotes. g. replace (' <text1b', ',="" '<text2b',="" 'text')="" 'true'.<="" a="" be="" false="" i="" it="" like="" must="" or="" oript="" return="" s="" string="" td="" then="" true="" value="" variable=""><td></td></text1b',>	
		V
var x='tr		. (?)
	<pre>=afe.executeSql('select count(*) from MySecurityTable</pre>	
	r_login = <%USER_LOGIN%> and bc_id =<%CURRENT_BC_ID%> and right="EDIT"');	
if (check		
[1 1013	2 ' ; }	
5 x; 7		
3		
9		
.0		
.1		
12		
L3		
L4		
15		
16		
17		
L8 L9		
20		
.0		
SYNTAX CHECK		
Verification OK		

ок	CANCEL

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

Paro Configuration Manager 3.779					
Show Application a	server Log				
e	Value				
	The same as the web security system				
	,	e Value	e Value		

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.

🛃 Apparo	Demonstration	Email connectio	n configuration - EMail
Basic settin	gs		
Connection nam	le	EMail The email connection name is the name that will be used in all of	• mail Import Business Cases.
Email address		qsdemo@apparo.solutions Only emails sent to this address will be processed and the address	• ess will be used for information messages sent to the original email sender.
Trusted email s	ervers	192.168.0.199, imap.apparo.solutions	rasses. If you don't love this field black then only emails received from the s

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.

Apparo Demonstration Bu	siness Case Designer - Email Import Business Case (EIBC) / Emai
Email import group settings	
Main group settings Business Cases Email texts	Security
Allowed email sender addresses	*@apparo.*
Security keywords	<%EMAIL_KEYWORDS%>
Email confirmation required	
Confirmation reply must come within	15 minutes
Check if the email address of the sender is defined in the local security syste	m 🖌
Authorized security groups	GROUP_1, GROUP_2
Business Case limited access	No limitation (default)
	Limited for all
	C Limited for variable value

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. <u>*@apparo.*</u> 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

Enter comma separated list of security g	roups for each Apparo role:
Apparo Client Administrator	ADMIN System Administrator
Apparo Connection Administrator	ADMIN System Administrator
Apparo Designer	ADMIN System Administrator, DEMO System Designer
Apparo Import & Export Administrator	ADMIN System Administrator
Apparo Portal Administrator	ADMIN System Administrator, DEMO System Designer

OK CANCEL

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.

P A	Paro Demonstration				Database	e connection (configuration
Main	Adva	nced	Variables	Automatic tables/columns	creation	Security	
Add all s	ecurity grou	ups that m	ust be able to us	abase connection then it is possible to restri e this database connections.	ict access to s	pecific designer us	ers.
If this set Security	2		fhen everybody of Group_A, Admi	can use this database connection.			
О	¢	CAN	ICEL				



3.4 Folder security

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

+ New	🖋 Edit	
Busines	s Case Folders	t
🔻 🗁 Demo	onstration	
🔻 🧁 м	laster Data (MDM)	
i i i i i i i i i i i i i i i i i i i	👅 test	
🧎 P	lanning	

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:

Name of this Business Case folder	Master Data (MDM)	
Description of this Business Case folder		^
		~
Necessary security group to see and open this folder	Securtiy_Group_A	^
		\sim
Necessary security group to edit/delete this folder	Securtiy_Group_B	^
		~
Necessary security group for running the included Business Cases of this folder and subfolders	Securtiy_Group_C	^
		\sim
Necessary security groups with limited access to Business Cases of this folder and subfolders	Securtiy_Group_D	^
		\checkmark

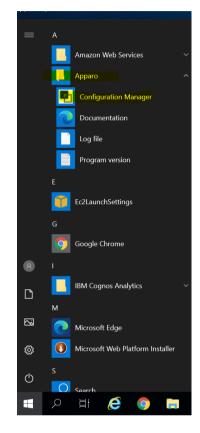


4 System administrator user security

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





Paro Configuration Manager 3.779				—	
File Windows Services					
📓 Save 💿 Test Config	iguration 🚺 🔕 Start Apparo 🕕 Show Application		ver Log		
Configuration	Name		Value		
Architecture	Authentication	Lo	Login page		
Application server	Security System		LDAP		
File system paths	LDAP host name		localhost		
🗐 Web security system	Use SSL		no		
i eMail security system	LDAP port		39		
Repository	Base Distinguished Name (DN	l) da	=apparo,dc=solutions		
🕍 License key	Authentication Method		mple bind		
	Bind user login		uid=admin, ou=system		
	Password		***		
	User Object Class		inetOrgPerson		
	User Name Attribute		cn		
	Group Object Class		groupOfUniqueNames		
	Group Name Attribute		1		
	Group Member Attribute		niqueMember		
	Web security groups for administrators		DEMO System Administrator		
		Test Security System	Test Security System Connection Test User Login		
	With Apparo it is possible to change sensitive data.				
Therefore it is important that authorized users can change data only.					

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".