Users access Management in BFC SYENSQO

---

1. OBJECTIVE AND SCOPE 🙂

1.1 Objective of this Procedure

The purpose of this document is to describe the process to **manage users accesses in the Security module** of BFC tool of SYENSQO Group , as well as to **execute the Internal Controls** related to the users management.

1.2 Scope

This procedure applies to the **BFC Administration** team.

---

2. REFERENCE DOCUMENTS

- Companies management (SYENSQO GAR List and BFC) (Finance Service Line)

---

3. DEFINITIONS

BFC - Business Financial Consolidation (Syensqo's Group Consolidation Tool)

BFC-Admin - BFC Administration Team in charge for the Administration of the BFC

GAR SYENSQO - Group Accounting Reporting Team (Consolidation team)

HR - Human Resources

IS Adagio - Team responsible to update the Active Directory Group (AD) list.

SLA - Service Level Agreement

FSL - Finance Service Line in GBS including Services Units, CAM and Accounting Platforms

CAM - Company Accounting Manager

RPA - Robotic Process Automation

---

4. SUMMARY

4.1 Principle and Context

It is **necessary to create and keep a user accesses in BFC aligned with user's position, responsibilities and needs**: either to enter the necessary information in the BFC reporting packages or to retrieve, analyse and validate the consolidated results.

Internal controls related to the process of users management have been defined to **guarantee a secured management of accesses**:

- BFC users are granted **accesses rights aligned with their responsibilities and needs** in the BFC reporting cycles,
- Any **new access** requested in BFC is **duly approved,**
- Accesses of **users who left** the group are **disabled,**
- **Inactive users** have their BFC account **temporary deactivated.**

Internal controls concerning access requests and users deactivation are described in the links below:

- **BFC-2.4 UAM05 Access Requests (previous SEC07)**
- **BFC-2.6 UAM06 Change of user access rights (previous SEC11/movers)**
- **BFC-2.7 UAM11 Deletion of user access rights (previous SEC11/leavers)**

3 type of risks related to BFC accesses:

- **High impact's risk**: insider dealing
- **Medium impact's risk:** modification of data on a legal company for which the user is not responsible.
- **Low impact's risk:** access for consultation to a legal company / Business in which the user should have no prior interest.

4.2 Responsibility

The BFC-Admin team is responsible to manage the user accesses in BFC, such as:

- Create or update BFC accesses,
- Request the approval from Consolidation Manager each time sensitive rights have to be granted to a user,
- Request to IT updates on BFC Active Directory list (list set up to allow SSO Single Sign On usage in BFC),
- Check active status of users in HR system,
- Guarantee compliance of users management with BFC Internal Controls (execute controls and store evidences),
- Support both Internal and External audit campaigns related to Internal Controls.

The **SLA (Service Level Agreement)** for requests **to create or update a user in BFC** is:

- **During Closing Periods:** 1 hour
- **Outside Closing Periods:** 1 day

4.3 Process Overview and Key Principles

Requests to **create a new user** or to **update the profile of an existing user** are **submitted by end users (or their direct managers) to BFC-Admin (SCo-$BFC-Admin) mailbox .**

Request for new user creation must include**:**

- the **manager of the end user** in copy in case he/she does not submit himself/herself the request - *if manager not in the loop of the request, the BFC team has to request a formal approval from him/her (this is part of Internal Control)*
- the **description of required rights** : scope of companies or Businesses, type of actions (data entry or consultation)
- **if possible,** existing user whose rights can be used as **reference/model** for the new user

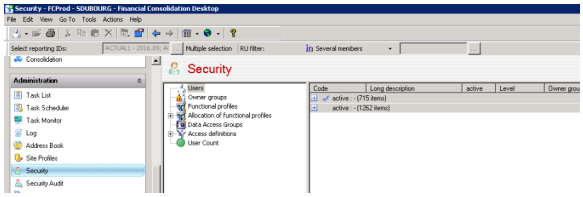
The **updates** can be:

- Change the existing rights (Functional Profile or Data Access Group) - the requestor needs to describe the change needed
- Reactivate a deactivated user
- Deactivate a user

The **compulsory information necessary to create a user** in BFC is:

- First name and Last Name
- Syensqo's network ID
- Email address
- Functional rights needed (scope of companies, editing or view rights...); or reference to the rights of an existing user fitting the needs of the requestor

The management of the users in BFC is performed directly in the **BFC_Prod_SCO** database / **Security** module within the **Administration** domain.



Security module covers:

- **Users**
- **Owner groups**
- **Functional profiles**
- **Data access groups**

4.3.1 Overview - Access Definitions

Each access in BFC is a **combination of:**

- **Owner Group:** used to allocate users in defined organizations/teams
- **Functional Profile:** Type of actions the user will be able to perform in BFC,: "editing" versus "read only" rights
- **Access Group:** Scope of data on which access is granted: segregation can be made by reporting category, by scope of legal companies and /or by scope of Businesses

---

4.3.2 Overview - Functional Profile

The **Functional Profile** defines the actions that the users can perform in BFC in each module: data entry in reporting packages, access for consultation, posting of journal entries, reopening of packages; consolidations run...

The main **Functional Profiles** in BFC are:

- **ADMINISTRATEUR** - BFC tool Administrators
  - can perform all the tasks in all domains. Has full rights, including the "Deletion" ones
- **ADMIN-GAR** - Limited ADMIN rights in addition to Consolidation rights
  - Restricted administrator rights -> publication of packages + Creation/update of filters
  - Provided to one member inside Consolidation team to support during closing process in case BFC Admin can not act
- **CONSOLIDEUR** - Consolidation rights
  - For the Consolidation team - versus other users, special rights to enter manual entries and to run consolidation
- **CONSO-SAISIE** - (limited people in US region)
  - For users combining access rights to fulfill packages and access rights to run regional consolidation for local compliance needs (US scopes)
- **AUDIT**
  - For people in charge for the internal/ external audit, who must be able to consult the whole application
- **SAISIE-RESTIT** - majority of accesses given
  - For users in charge to enter data in the Packages: Local accountants, FSL Service Units, CAM and Accounting Platforms teams
- **ADMIN-IC-SBS**
  - For users in charge for the Intercompany reconciliation process (mainly Interco team in service Unit "financial accounting" from FSL). Access in display mode to Dimension builder needed to allow the technical automated interface from BOIC.
- **RTR-BO-COR**- Same rights as SAISIE-RESTIT + Rights to reopen packages
  - Transversal teams in FSL (limited people) monitoring reporting process and coordinating corrections (thus having rights to proceed package re-openings)
- **REOPEN-DEROG** - same rights than RTR-BO-COR + Rights to publish by derogation
  - Limited transversal teams coordinating corrections (package unlockings) and publication by derogation (special permission)
- **RESTITUTION**
  - For people whose access is restricted to consulting rights: Business Controlling community mainly consulting and running reports
- **RESTIT-PACK**
  - Same as RESTITUTION, with addition of display rights to the Package Manager
- **ROBOTS**

    - To allow each robot user perform multiple automated actions: Import SAP interfaces / BFC databases monitoring / Package re-openings
- **IT**
    - For BFC technical administrators taking care of BFC servers and application monitoring - display rights only

Some of these **Functional Profiles (ADMINISTRATOR / CONSOLIDEUR / CONSO-SAISIE / RTR-BO-COR / REOPEN-DEROG)** can be considered as **sensitive**, because they allow to perform critical actions in BFC, as:

- Change the customizing of BFC objects
- Manage and Consult Journal Entries at Consolidated level
- Create; update; run; lock and unlock Consolidations
- Unlock packages (Reopen packages Published in Standard mode)
- Unprotect packages (Reopen packages published by Special Permission)
- Publish by Special Permission (Publish packages with errors)

The creation of a user with a sensitive Functional profile **must be formally approved by the Syensqo Consolidation Manager**.

Internal controls concerning BFC Functional Profiles and their access rights are described in the link below:

- **BFC-2.2 UAM04 Functional Profiles (previous SEC 03)**
- **BFC-2.3 UAM07 Matrix of incompatible functional profiles (previous SEC-04)**

4.3.3 Overview - Data Access Group

The **Data Access Group** defines the **Reporting Categories** that will be granted, the L**evel of the data** (From local package till Final consolidation) that can be reached in each category, and the **Scope of data** (legal companies versus Businesses).

The definitions are based on:

- **Reporting Categories**
    - **ACTUAL0** - Shareholding data / Appendices on Non Conso companies
    - **ACTUAL1 -** Pillar II and CBCR collections
    - **ACTUAL1-TAX** - Quartertly Tax reporting
    - **ACTUAL2** - IFRS Financial Statements Consolidation
    - **ACTUAL3** - Quarterly appendices to ACTUAL2
    - **PREV** -Budget reporting (Corporate Controlling purposes)
    - **RSB** - Restatement of Y-1 IFRS FS (External communication purposes)
- **Level of Access to each Category**
    - **Data entry access** -access the data in local reporting packages
    - **Data analysis access** - access the data in Reports
    - **Consolidation access** - access to consolidated data
    - **Central manual journal entry** - access the journal entries
- **Definitions of view (most used)**
    - Reporting Unit - Legal companies the user will have access to
    - Activity1 (Market) - Business dimension the user will have access to (for Sales - P&L - Acc Receivables indicators)
    - Activity2 (CGU) - Business dimension the user will have access to (for Fixed assets - Investments - CAPEX - Acc payables indicators)

Note that the **Reporting Units** are in **most of cases defined using filters** when the user needs to access to multiple companies.

While **Businesses** are in the majority of cases **defined using filters based on GBU's** "Global Business Unit " level when the user needs to access to several Activities 1&2 belonging to the same GBU he/she is working for.

4.3.4 Overview - Authentication

Two types of **Authentication** (User ID and Password):

- **External** - Linked to SSO Single Sign On (Syensqo Network User ID and Password also applies to access to BFC).
- **Internal** - Not linked to Single Sign On (same user ID as for Syensqo network but temporary Password).

To comply with **Syensqo Security rules, a user must be created with External Authentication.**

Limited exceptions (access created with Internal authentication) can be authorized (but such cases have always to be challenged by BFC Administration team as they do not comply with Syensqo Security rules):

- The user needs a **second profile** (2 kind of responsibilities or temporary transition from existing position to a new one requiring 2 different functional profiles)- A user can only have one access with SSO.
- The user is **located outside the Syensqo Network**.

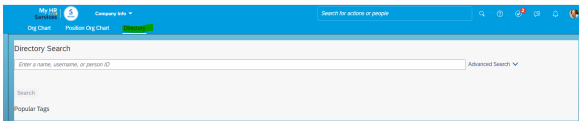
The users with the **Internal authentication** will have to manage the password directly in BFC.
They will need to **change it every 90 days** and request to the BFC Admin team to reset their password in case of issue.

---

5. VALIDATE THE USER STATUS IN THE HR TOOL

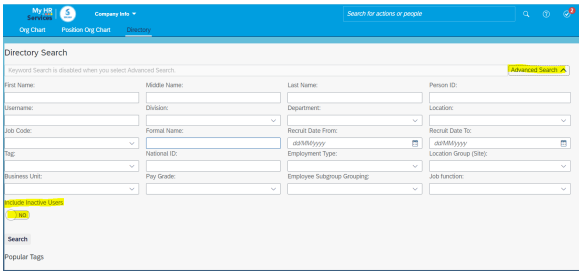
Before creating a new access, BFC Administration team must **1st check that the user has an Active status in HR system**

To access the search feature in Org. Chart, use the following link: https://hcm-eu30.hr.cloud.sap/sf/liveprofile?bplte_company=syensqo&_s.crb=uly6aj5olRnKfSxHH1pm1sNqYeeAOvyZ5v%252fTlKIJGNA%253d



Click on **Advanced Search** if you need to use other search criteria.

If you don't find the user you're looking for, **include inactive users** in your search.

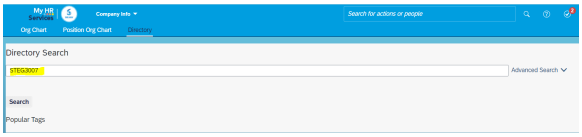


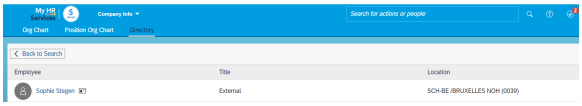
The user can be inactive because:

1) he/she doesn't work for Syensqo group anymore **BFC access shouldn't be granted**.

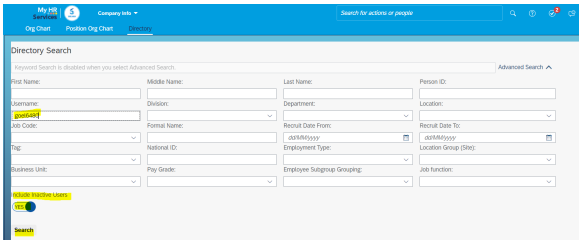
2) the onboarding process is not finished yet **The date for granting access to BFC should be agreed with her/him manager.**

Enter the **username** or **name** and click on **Search**





Example of Inactive User

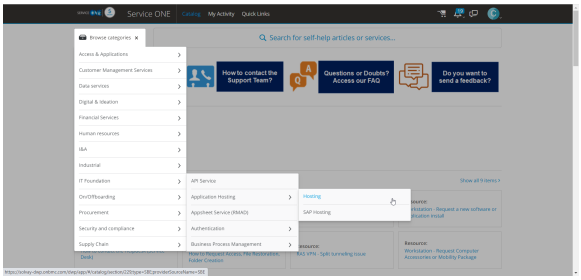


6. REQUEST TO ADD THE USER IN THE ACTIVE DIRECTORY GROUP

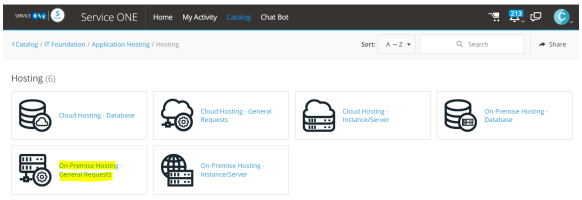
After ensuring that the user is active in the Group, it has to be requested to include the user in the **Active Directory Group**. This will **allow the activation of the SSO** (Single Sign On) : synchronization of BFC user ID and password with Syensqo network ones

To request to add the user to this directory, BFC Admin needs to create one **ticket in Service One**

https://solvay-dwp.onbmc.com/dwp/app/#/catalog

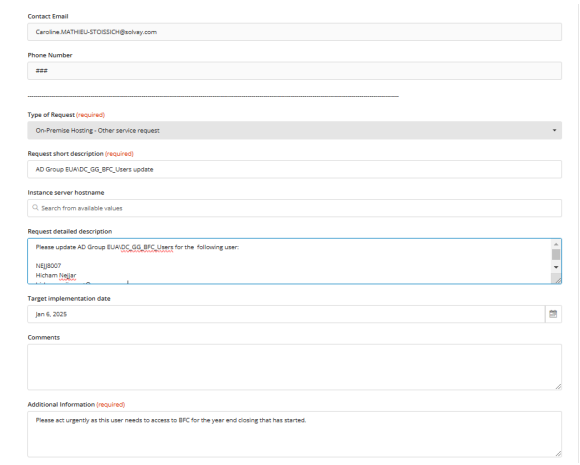


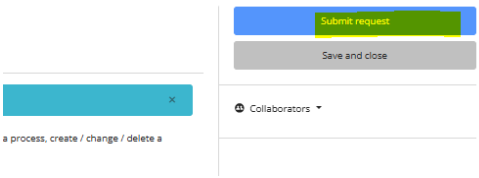
IT Foundation Application Hosting Hosting General Requests



Several fields to complete:

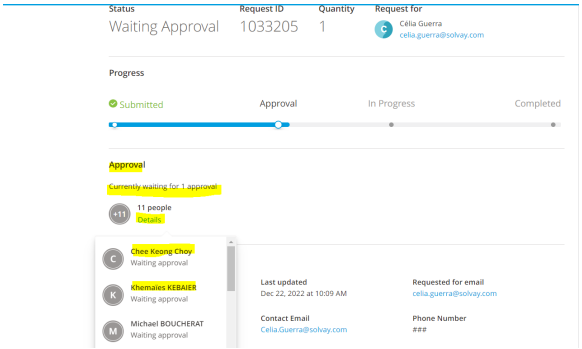
- **Type of request -** Other Services Request
- **Request short description** - AD Group EUA\DC_GG_BFC_Users update
- **Request detailed description :** define which AD Group has to be updated and insert details of about user - *below example* :
- *Please update AD Group EUA\DC_GG_BFC_Users for the following user:*
    - *NEJJ8007*
      Hicham Nejjar
      hicham.nejjar-ext@syensqo.com
- **Target implementation date :** select the day of the request to ensure the team will act quickly
- **Additional information** - "no additional info" / when the access is urgent (on going closing) this is to be mentioned (*see example*)





Press **Submit Request** button

NOTE: In case the request is not answered within 2 days, we should get in direct contact with one of the Approvers and ask for feedback and urgent response.



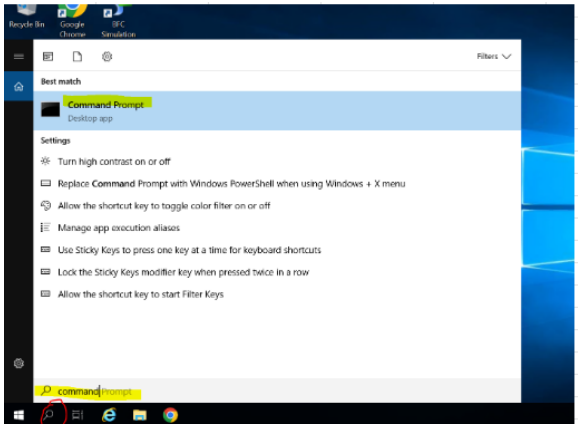
7. CHECK USER ID's IN ACTIVE DIRECTORY GROUP "DC_GG_BFC_Users"

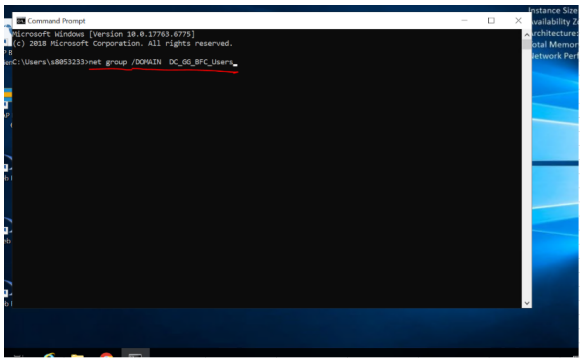
When **user ID is included in this AD Group**, it means that **SSO is activated**

Active Directory Group "**DC_GG_BFC_Users"** is the one that we indicate **in our Service One requests to activate SSO**

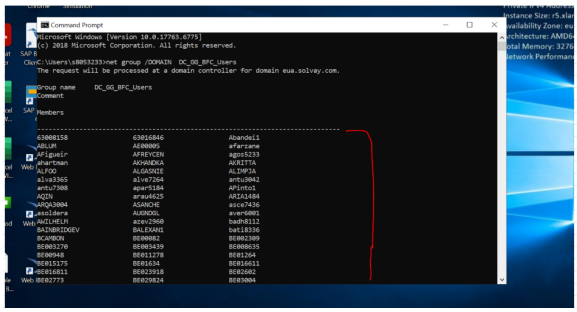
This check is very **useful when a user has his account activated in BFC but he tells us that he cannot connect**, receiving an error message of the type "user name and/or password invalid" => if we **cannot find the user in this list,** then this **confirms that DT has deleted the SSO** with BFC => we must therefore **submit a request in Service One to add back the user** in this Active Directory Group

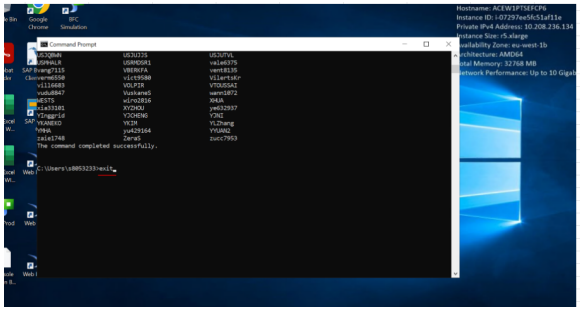
Step 1: in Search field Windows enter "Command Prompt"





Step 2 in window "Command Prompt", enter "net group /DOMAIN DC_GG_BFC_Users" + press ENTER





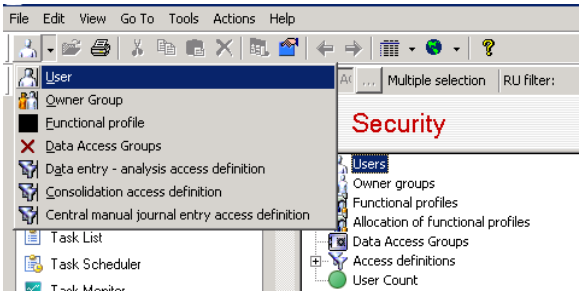
Step 3: in window "Command Prompt", the list of User ID's included in the Active Directory Group BFC is displayed

Step 4: in window "Command Prompt", to exit the command enter "EXIT" at the end and press ENTER => the window will be automatically closed

---

8. CREATE THE USER IN THE BFC

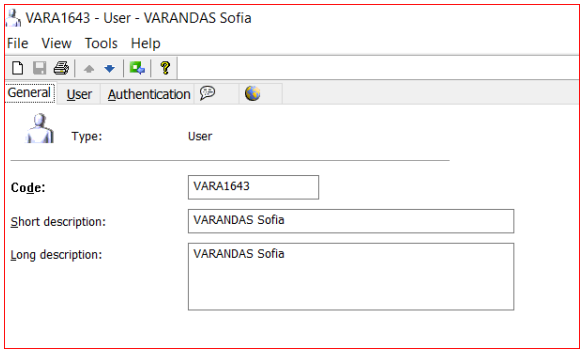
Once confirmation received of creation of the new user in the Active Directory Group (step before), in the **Security module** go to the option **New User.**



Note: when request applies to RPA (Robots or RPA developers), please **refer to section 10.3 Other Actions - RPA and DT users** to apply the specific creation rules for this category of users

In the tab **General** enter:

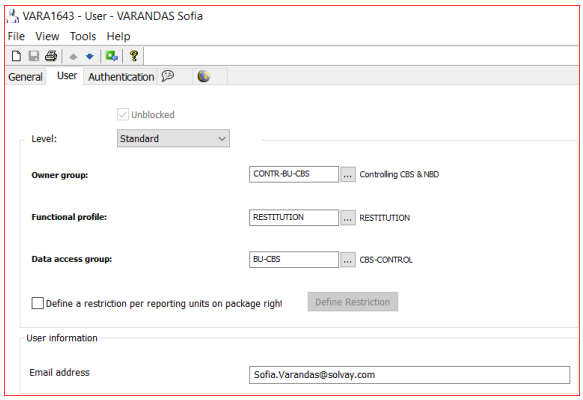
- The **Code** - BFC ID (= SAP user ID available in the HR Success factors).
- The **Short description** - LAST NAME and First name.
- The **Long description** - LAST NAME and First name.



In the tab **User** enter:

- The **Owner Group**.
- The **Functional Profile**.
- The **Data Access Group**.
- The **E-mail address**.

In this example the user is a Business controller from CBS GBU requesting display access (RESTITUTION) on GBU results.



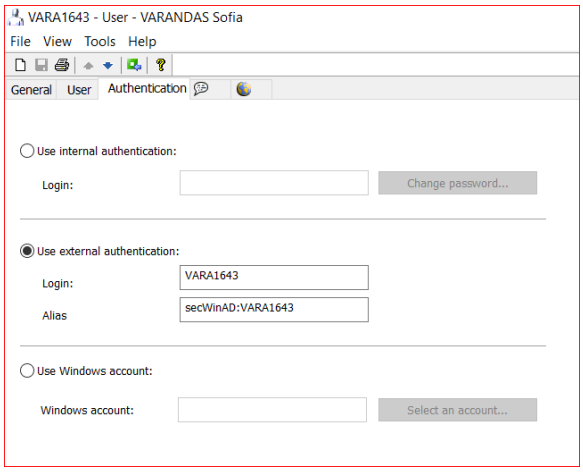
In the tab **Authentication** select if the user's authentication is **Internal** or **External**.

Note that **External authentication is the standard option.**

Note that for **Internal authentication** it has to be defined a temporary password, thus select the option "**Change password...**"

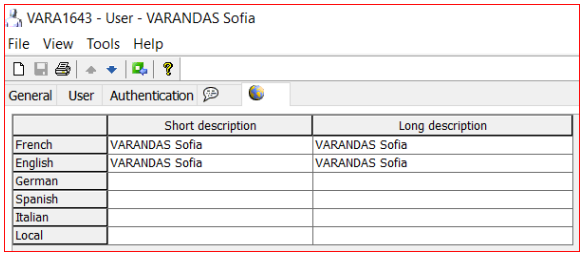
The rule to define a password is to enter "Syensqo" + DDMMYYYY *(DD MMYYYY being the day date on which the internal pwd is defined).*

Example: ***Syensqo04012024 if internal pwd is defined at that date***



In the tab **Translation** enter the full name of the user (LAST NAME First Name), in French and English, Short and Long descriptions.

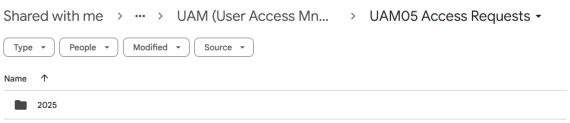
Then **Save** it.



	Short description	Long description
French	VARANDAS Sofia	VARANDAS Sofia
English	VARANDAS Sofia	VARANDAS Sofia
German		
Spanish		
Italian		
Local		

Refer to BFC-2.4 UAM05 Access Requests (previous SEC07)

The **chain of emails including the initial request and the necessary approvals** should be printed into a pdf and **stored in the BFC Internal Controls folder** for audit evidences purposes: UAM05 - Access requests



9. USER DEACTIVATION

Triggering events requiring a deactivation of a user access :

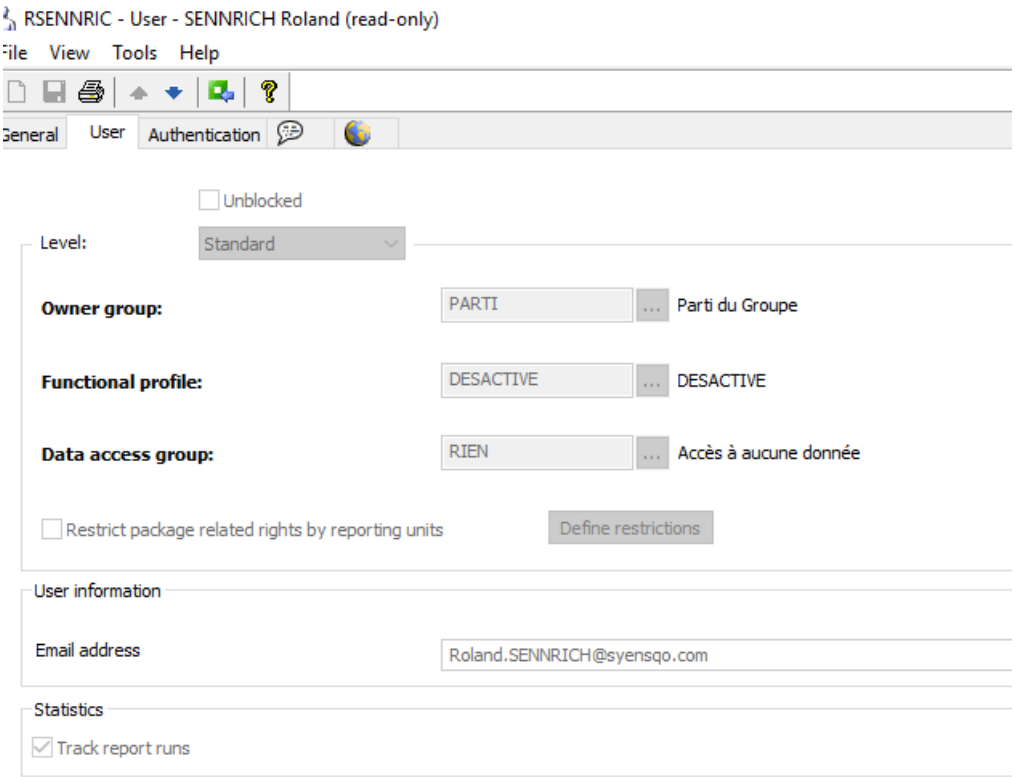
- **leave from Syensqo Group**
- **change of position** (internal move) **not justifying anymore a BFC usage**

How the request will be **come to BFC Admin team ?**

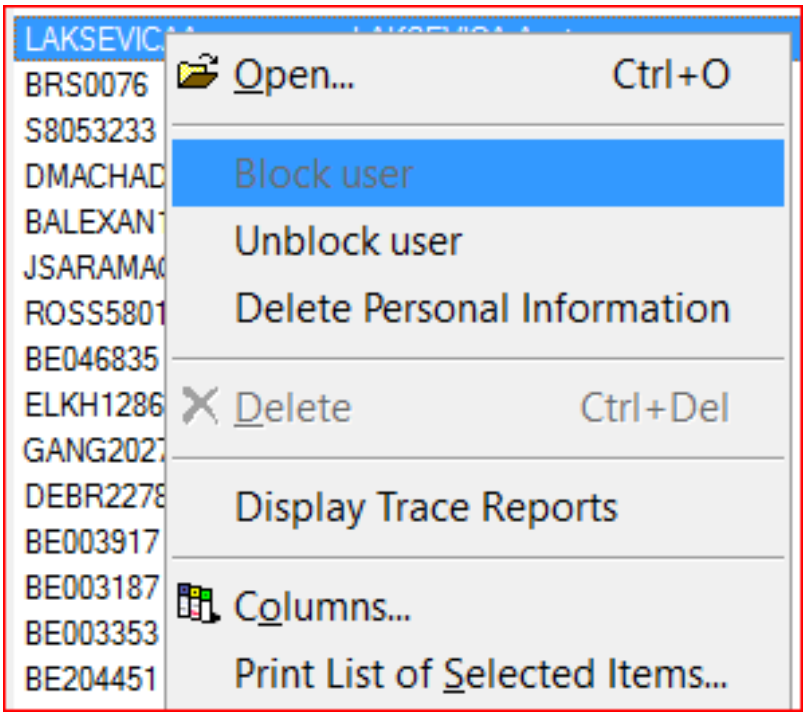
- through a **direct request by e-mail :** can be raised by the user him/herself, by any Finance members being aware of an internal move (not requiring anymore the usage of BFC) or a leave from Syensqo Group
- through a **notification from MyID**
- **through Internal Control procedures:**
  - BFC-2.6 UAM06 Change of user access rights (previous SEC11/movers) Deactivation done on a regular basis for movers monitoring changes in HR databases
  - BFC-2.7 UAM11 Deletion of user access rights (previous SEC11/leavers) Deactivation done on a regular basis for leavers monitoring changes in HR databases
  - BFC-2.8 UAM12 Periodic review of inactive users (previous SEC12)Temporarily deactivation on BFC when the user has not connected during the last 6 months

In BFC "Security/Users" module, deactivation will be proceeded the following in the user profile:

- Owner Group: PARTI
- Functional Profile: DESACTIVE
- Data Access Group: RIEN



and the user must be **blocked** in order to be prevented from accessing BFC.



10. MANAGEMENT OF OTHER OBJECTS IN THE SECURITY MODULE

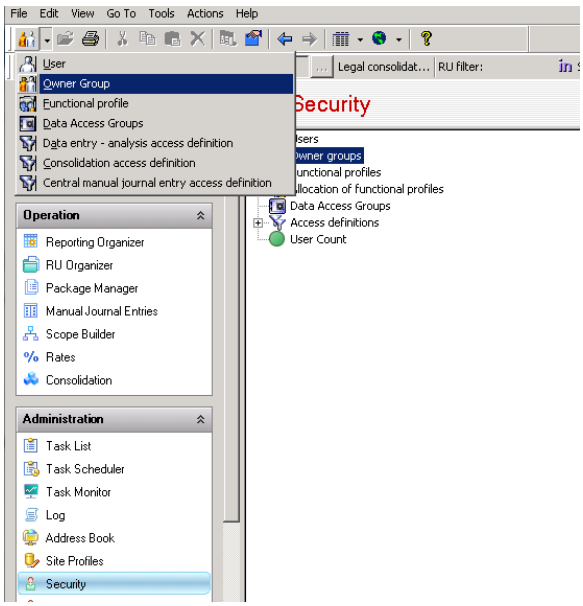
10.1 Management of Other Objects in the Security Module - Owner Group

The creation of a new **Owner Group** may be necessary when there is a new organisation team in the Group.

As example, in 2023 with the PO2 spinoff project of Solvay Group, **new owner groups (ECO-xxx and SCO-xxxx) were created to allocate the users between both future Groups Solvay (ECO) and Syensqo (SCO)**

The management of the Owner Groups is done in the Security module within the Administration domain.

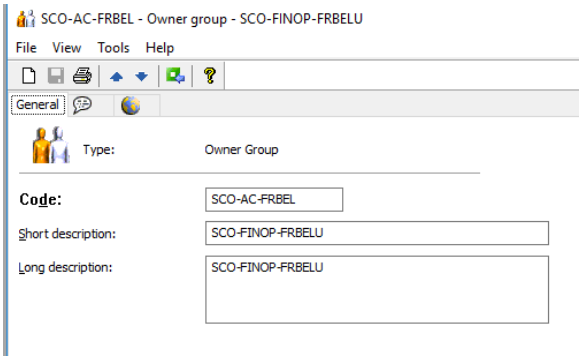
The creation of a new owner group can be done through the option "**New Owner Group**".



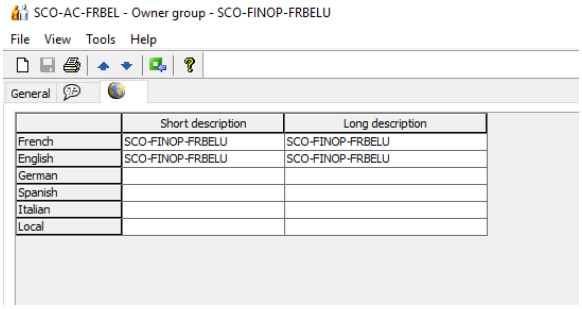
In the tab **General** enter the:

- Code.
- Short description.
- Long description.

In this example, it was determined the Code and the Descriptions as "**SCO-AC-FRBEL" and "SCO-FINOP-FRBELU"**.



In the tab **Translation** enter the description either in Short and **Long description** for **French** and **English** languages.



10.2 Management of Other Objects in the Security Module - Functional Profile

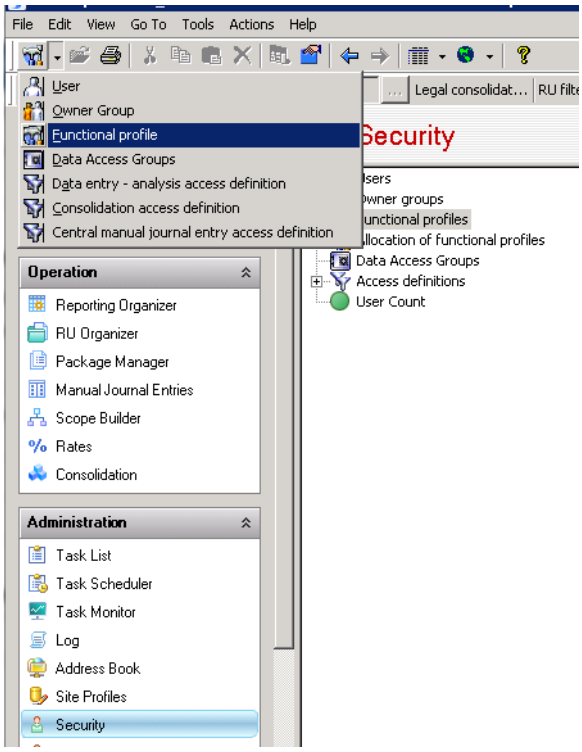
It might be necessary to create or update a **Functional Profile** when there is a new need for a group of users.

The creation or the update of a Functional Profile **must be formally approved by the Syensqo Consolidation Manager** referring to **BFC-2.2 UAM04 Functional Profiles (previous SEC-03)**

The management of the Functional Profiles is done in the Security module within the Administration domain.

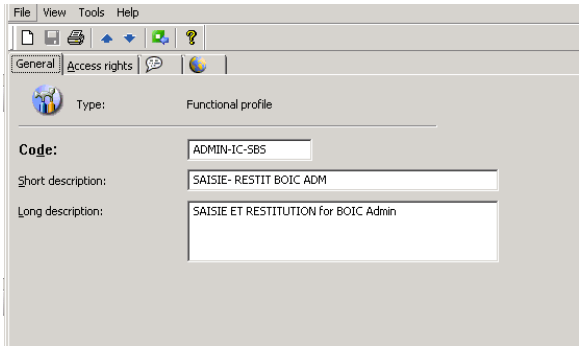
A new Functional profile can be created from the scratch in the option "**New Functional Profile**", or through the "**Save as**" from another one.

To update an exist Functional Profile open it and perform the necessary changes.



In the tab **General** enter the:

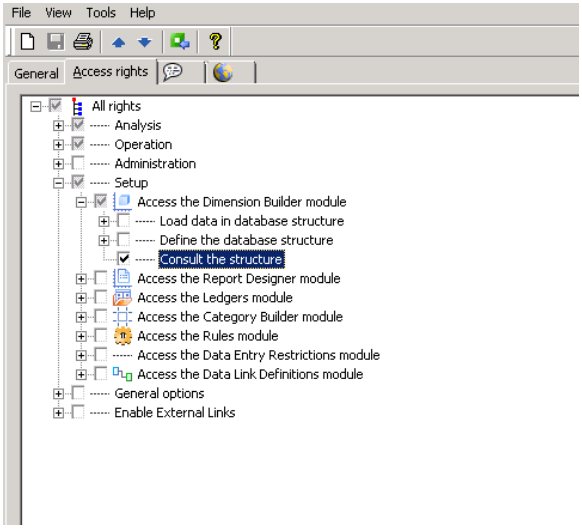
- Code.
- Short description.
- Long description.



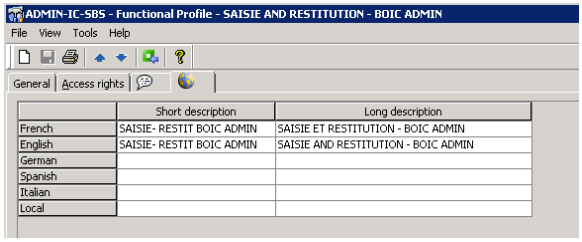
In the tab **Access Rights** selection the actions that the users will be able to perform in each of the following domains:

- **Analysis** - Schedules, dashboards and reports (organization and execution).
- **Operation** - Management of reporting sessions.
- **Administration** - Management of Tasks, Security, Log & Monitoring.
- **Setup** - Customization of the BFC: Category Scenario, Set of rules, Documents.
- **General Options** - Miscellaneous.

In this example, it was requested to create a new Functional Profile for the BOIC Team, with reference to the Functional Profile SAISE-RESTIT. The new profile should enable the users "Consult the structure" in the domain Setup.



In the tab **Translation** enter the description either in Short and **Long description** for **French** and **English** languages.



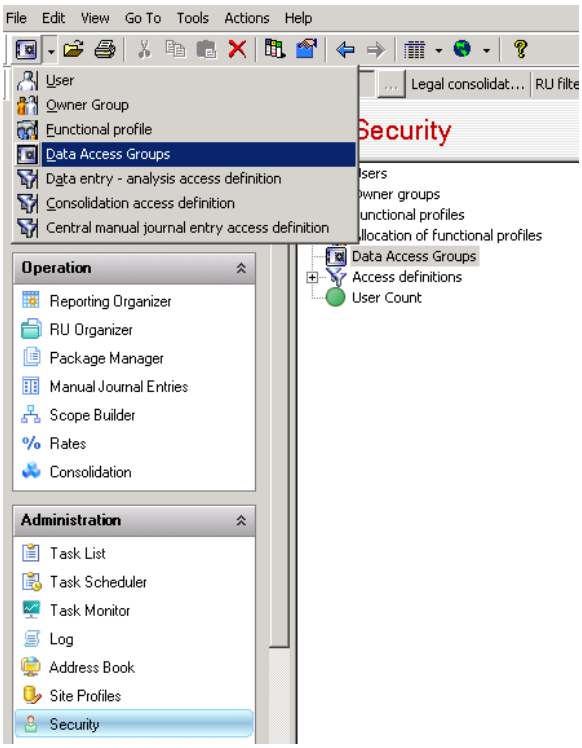
10.3 Management of Other Objects in the Security Module - Data Access Group

A new **Data Access Group** should be created when there is a specific need for a group of users and there is any that meets the needs.

As example, in 2023 with the PO2 spinoff project of Solvay Group, **new data access groups (ECO-xxx and SCO-xxxx) were created to allow data segregation between both future Groups Solvay (ECO) and Syensqo (SCO)**

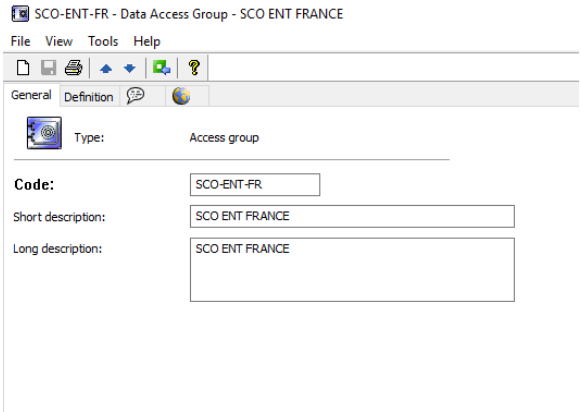
The management of the Data Access Group is done in the Security module within the Administration domain.

A new Data Access Group can be created from the scratch in the option "**New Data Access Group**", or through the "**Save as**" from another one.



In the tab **General** enter the:

- Code.
- Short description.
- Long description.



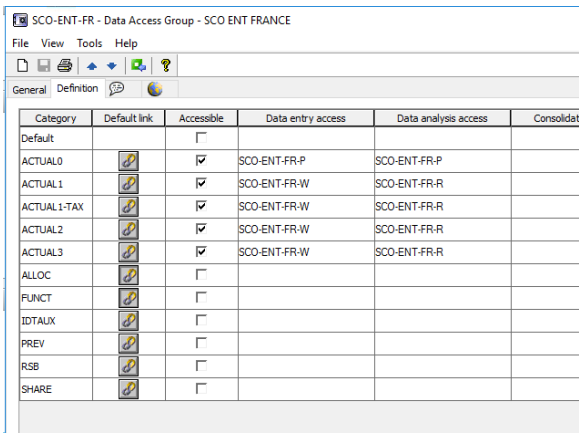
In the tab **Definition**, it has to be defined the **categories** that will be allowed to access, the **level of the data** that can be reached in each category, and how it can be accessed (In the Packages or in the Reports).

In the column "**Accessible**" flag the **categories** to be accessed, and then inform the Data Definition in the level of information that should be reached.

In this example, the Data Access Group "SCO-ENT-FR", allows to access the categories:

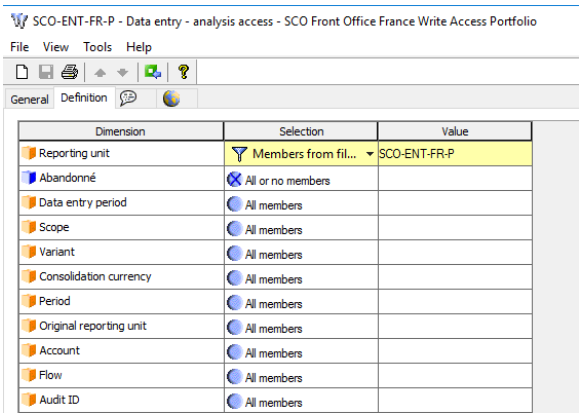
- **ACTUAL0**
- **ACTUAL1**
- **ACTUAL1-TAX**
- **ACTUAL2**
- **ACTUAL3**

And the level of information that can be reached is the Package Data, according to the definitions in the columns **Data Entry Access** (Package s) and **Data Analysis Access** (Reports).



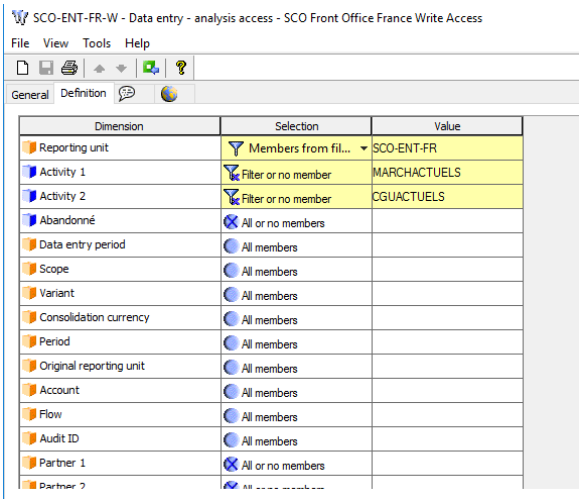
In this Data Access Group, 3 Data entry access & analysis had to be created:

- **SCO-ENT-FR-P** - Portfolio (for shareholding reporting in ACTUAL0 category)
    - It is based on dedicated RU filter "SCO-ENT-FR-P" including companies from FR "France" but also companies/affiliates from other countries (manually added) owned by FR cnies and for which FR teams have to complete ACTUAL0 packs (no local accountant to take care of ACTUAL0)



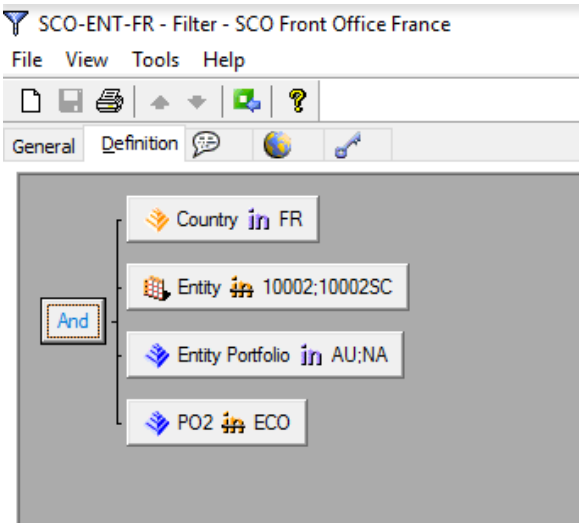
- **SCO-ENT-FR-W** - Write Access
- **SCO-ENT-FR-R** - Read Access

    - What defers in Write and Read definitions is that the SCO-ENT-FR-W has restrictions in the Activity1 and Activity2.
    - Both definitions have the same criteria for **Reporting Unit**: a filter name SCO-ENT-FR.



The **filter in the Reporting unit restrict the access to the companies** in France from Syensqo (SCO)

If it is necessary to create or update a Filter of Reporting Units see the topic in the following section



---

11. OTHER ACTIONS

11.1 Other Actions - Management of a Filter of Reporting Units

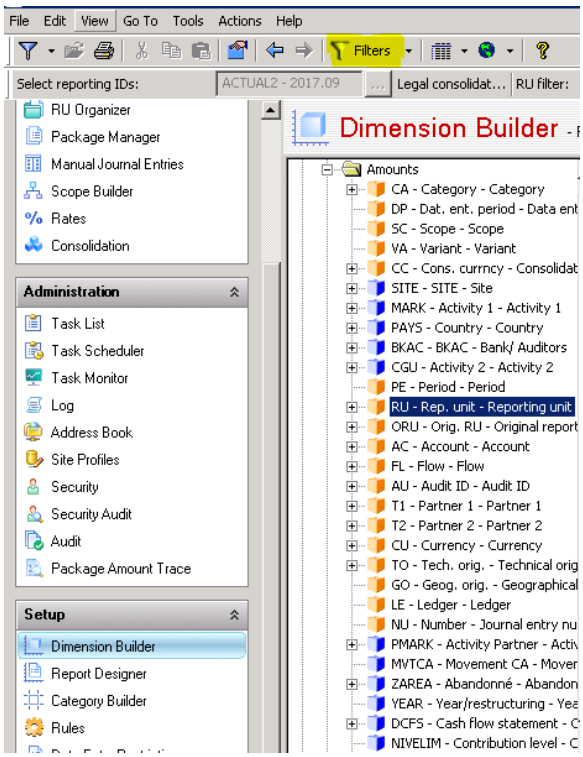
A filter of Reporting Units defines a **group of legal companies** to which a user can access to. **Cases driving the need to create or update** filters on Reporting unit:

- new team in charge for a group of companies => filter to be created
- new company acquired or change in consolidation method => filter to be updated

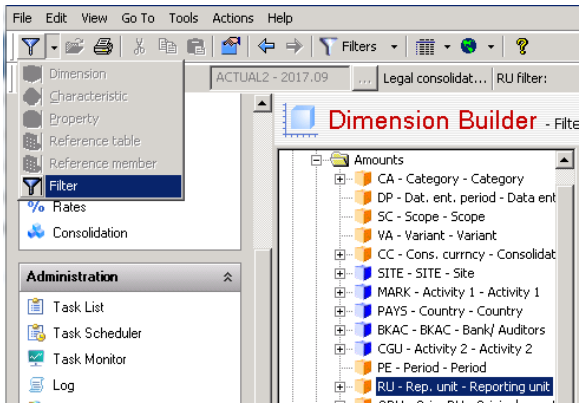
---

The management of a **Filter of Reporting Units** is done in the module **D imension Builder** within the **Setup** domain.

Change the Functional Mode to "**Filters**" view.

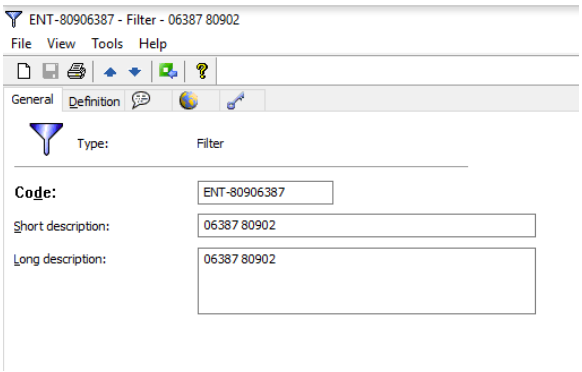


A new **Filter** can be created from the scratch in the option "**New Filter**", or through the "**Save as**" from another one.



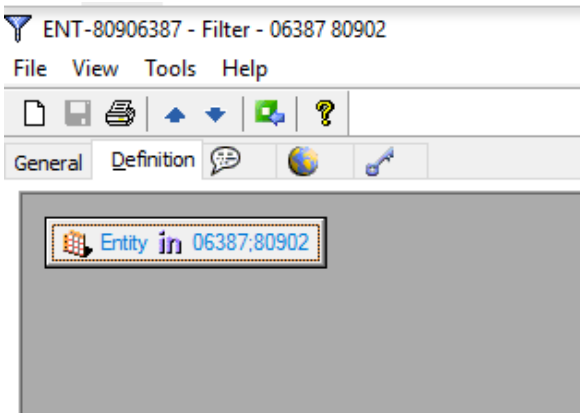
In the tab **General** enter the:

- Code.
- Short description.
- Long description.



In the tab **Definition** enter the criteria of the filter:

This example the filter is quite simple, it just allows the view for the companies **80902** and **06387**.



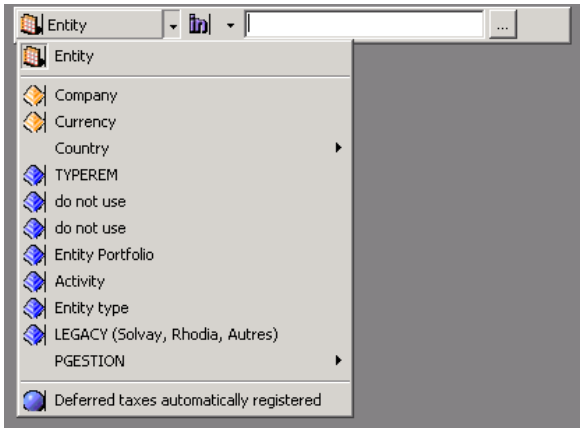
It is **preferred to create each time it is possible in dynamic filters** - pr eventing from manual maintenance - using the following criterias and fucntionalities.

- **The Operators:**

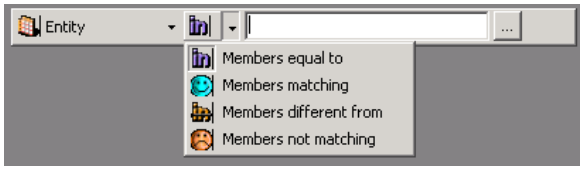
Insert operator AND

Insert operator OR

- **Other Dimensions**



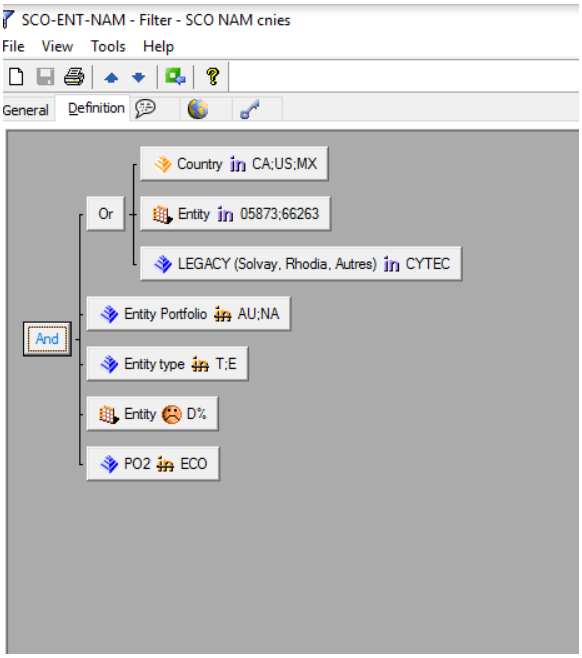
- **Types of Matching**



As example the filter created for the North American Entities that was defined:

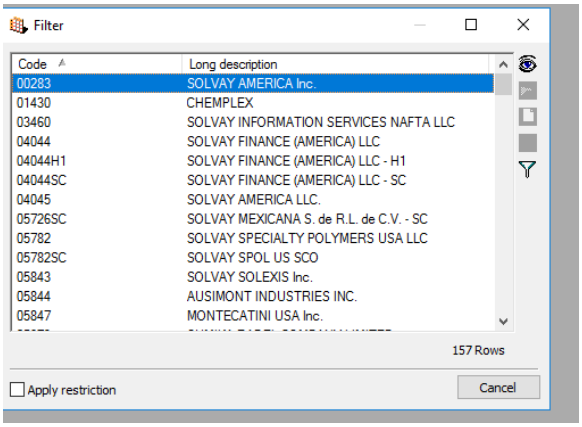
- **Country** CA (Canada) + US + MX (Mexico)
- **Or** companies equal to 05873 or 66263 (not located in the 3 countries above CA US MX)
- **Or** companies belonging to the CYTEC legacy (and not loocated in the 3 countries CA US MX and not equal to 05873 or 66263)
- **And** the entities having a portfolio not qualified as Others" or "Not applicable"

- **And** the entities not being Technical ones
- **And** the entities different than D% (the % defines that any character after the D, then it filters any company that starts with Dxxxx)
- **And** the entities not belonging to Solvay Group (ECO), but to Syensqo Group

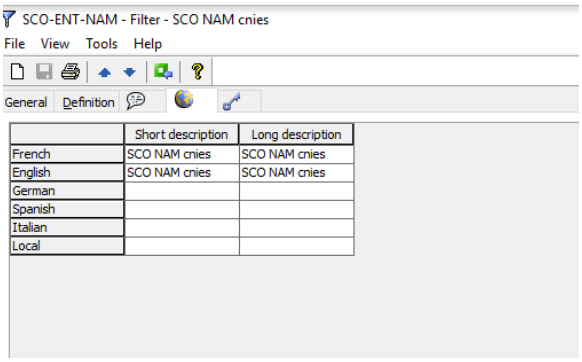


By click on the icon  Test Filter, it shows the companies that are considered in the Filter.

In this filter 53 companies matched the criteria defined.



In the tab **Translation** enter the description either in Short and **Long description** for **French** and **English** languages.



11.2 Other Actions - Update the Finance contacts in the GAR SYENSQO List of Companies

Through the requests received from end users to create or adapt their BFC accesses, BFC Admin has to **think about the possible consequences on Finance contacts listed in the GAR SYENSQO list of companies.**

Please refer to the GAR SYENSQO list procedure for maintenance

Examples: a new user telling he is the CAM of a company (or CAD or TCM or Acc Platform leader...) has to be declared as such in the GAR SYENSQO list.

11.3 Other Actions - RPA and DT users

RPA (Robotic Process Automation) users can be classified in 2 categories:

- **Robots** - Users corresponding to computers emulating humans actions. These users are created in BFC_Prod_SCO (same procedure as for human users).
- **RPA developers** - RPA team members may request access in BFC in order to develop business process automation that will be executed by robots.

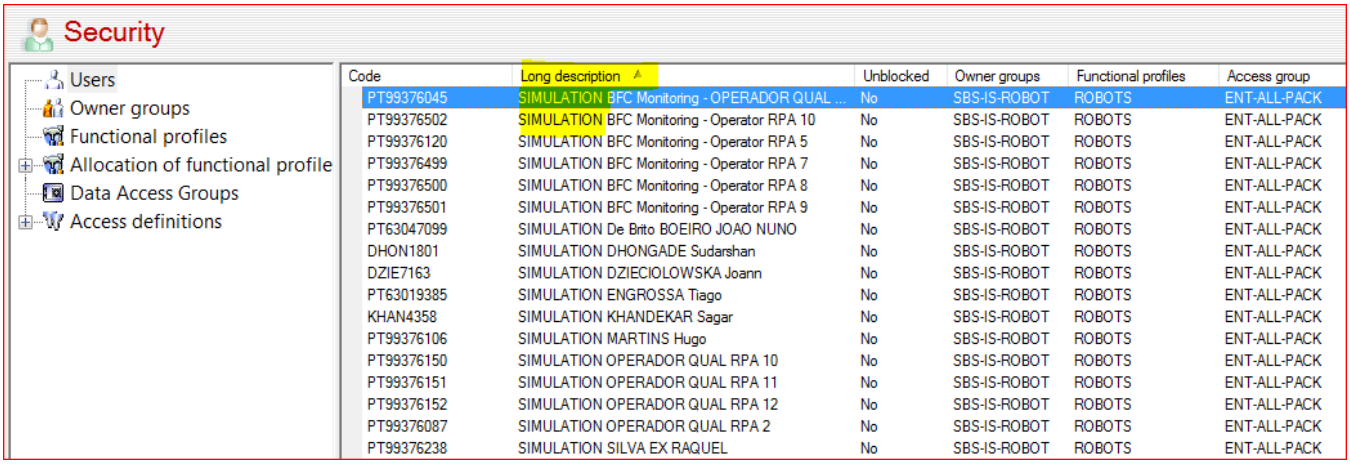
These users should have access to Simulation database (BFC_Prod_SCO_D4) only but since BFC_Prod_SCO_D4 is refreshed with a dump from BFC_Prod_SCO every month, we create these users

1) in **BFC_Prod_SCO with inactive** status and

2) in **BFC_Prod_SCO_D4 with active** status and

3) we **reactivate them in BFC_Prod_SCO_D4 every month** once the refresh has been concluded and upon request from RPA developers.

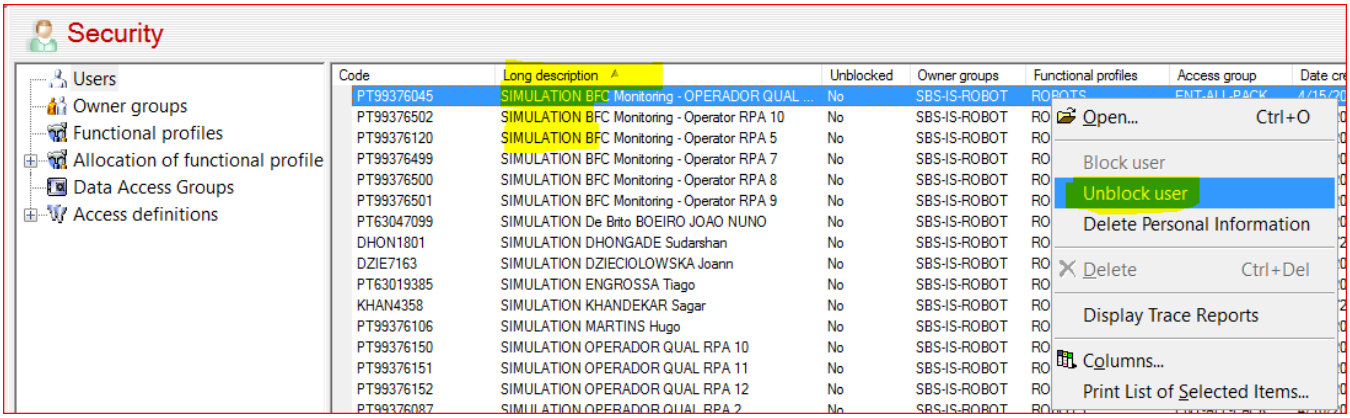
In order for these users to be easily identifiable, they should be created with the word "SIMULATION" at the beginning of the description.



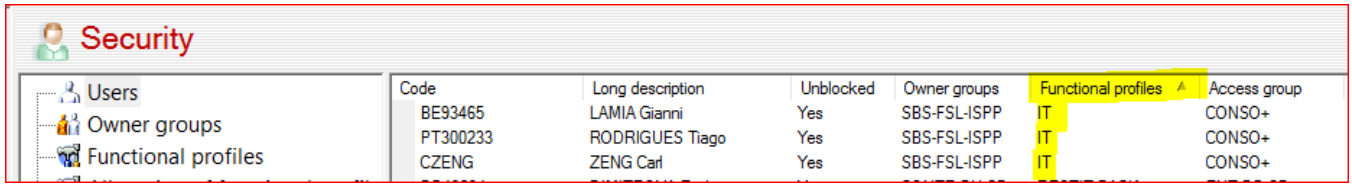
In BFC_Prod_SCO, **DT users** have their own Functional Profile (IT) and should be assigned to CONSO+ access group while in BFC_Prod_SCO_D4 they should be Administrators.

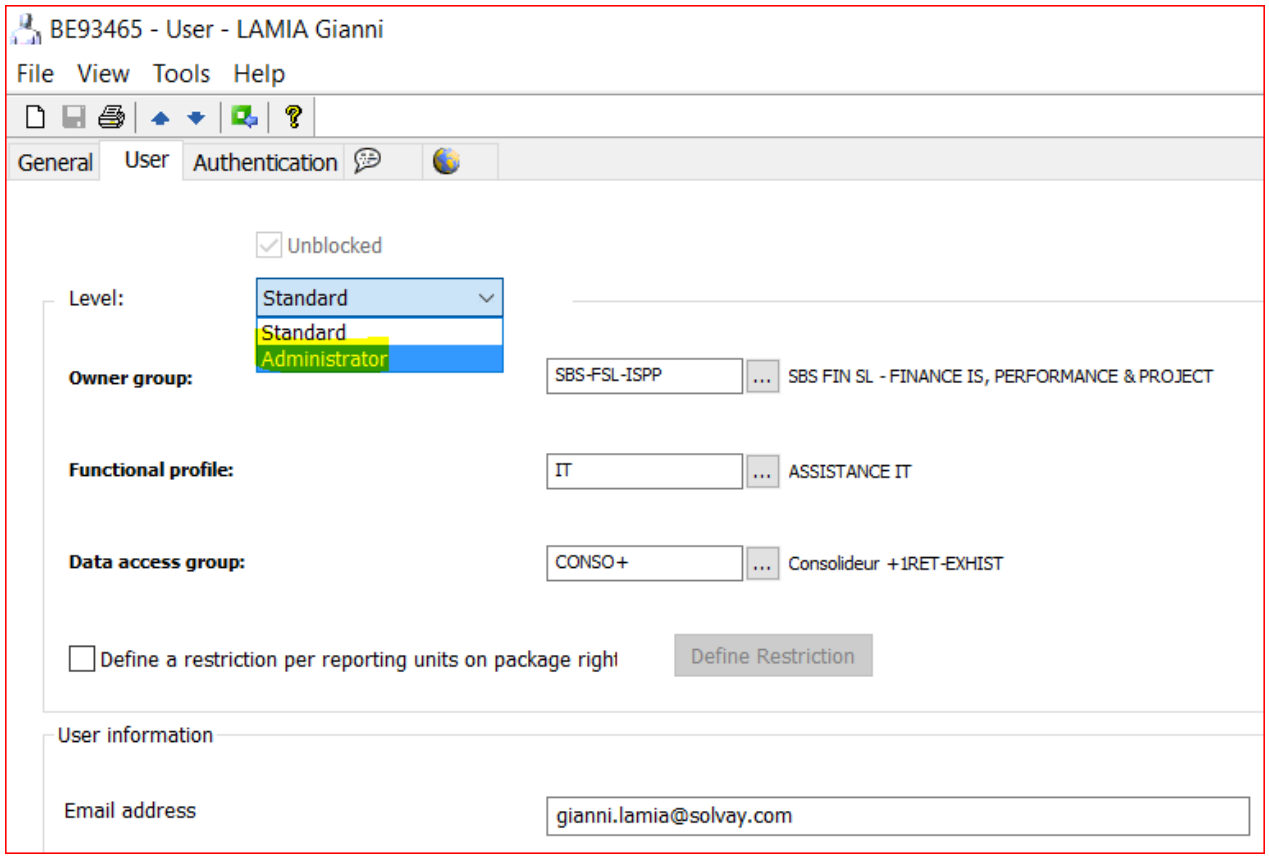
Once the **monthly refresh** has been concluded,

RPA developer users should be unlocked:



and **IT users should be changed to Administrators level:**





END OF THE PROCEDURE.