

SAP Business Objects Analysis for MS Office Authorization Strategy

Version: Final

Table of Contents

1	SAP BusinessObjects Analysis Authentication and Authorization	3
1.1	User types	3
1.2	Broad Category of Tasks in Business Objects Analysis	4
1.3	BW Authorization	4
1.4	Business Objects Authorization	5
1.4.1	Assignment of User Groups & Roles to the Folders in Business Objects in CMC	7
1.4.2	Relationship between Access Levels and User Groups in Business Objects CMC	8
2	Authorization Strategy	10
3	Step-by-Step SAP BusinessObjects Authorization Configuration	12
3.1	User and User Group Creation:	12
3.2	STEP 1: Creating a User:	12
3.3	STEP 2: User Group Creation	13
3.4	STEP 3: Importing Roles from the backend SAP BW system	14
3.5	STEP 4a: Automating Importing of Roles from SAP BW system into Business Objects	16
3.6	STEP 4b: Schedule a SAP Authentication Role update in Business Objects using a java program	16
3.7	STEP 5: Standard Access Levels	18
3.8	STEP 6: Custom Access Levels	19
3.9	STEP 7: Folder level Security	20
4	Top Level / Server Level Security:	24
5	Application Level Security:	26
6	Manage CMC User Security	27
7	Advance Rights	29
8	Security Query	31
9	Appendix (BW Authorization Set up in Detail)	33

1 SAP BusinessObjects Analysis Authentication and Authorization

- **Authorization** is the process of verifying the user has sufficient rights to perform the requested action upon a given objects.
- **Action** means to view, refresh, edit, schedule, etc.
- **Object** means: folder, report, instance, universe, etc.
- Authorization is handled based on how the “**access level**”, “**application security**”, and “**content security**” such as users and groups, universe security, folder access, etc. are defined using CMC.

SAP BusinessObjects Authorization works differently but in conjunction with SAP BW Authorization model.

SAP NetWeaver BW	SAP BusinessObjects Enterprise	Comment
Authorization Objects	Rights	Individual actions and activities that can be performed for an object
Profiles	Access Levels	A collection of activities and actions
Analysis Authorizations	Profiles	Controls access to specific dataslices E.g., Country = USA
Worksets	Folders	A collection of objects, reports, and documents
Roles	Groups	A collections of users who share the same account privileges. Both SAP and SAP BusinessObjects support a hierarchy of roles or groups.

1.1 User types

User Type	Task	Access Requirement
BEX Query Developer Business Objects Analysis Report Developers	<ul style="list-style-type: none"> ➤ Develop the source queries using SAP BW-BEX. ➤ Develop the reports in SAP BusinessObjects Analysis for excel. 	In order to develop a report in SAP BusinessObjects Analysis for excel ; <ul style="list-style-type: none"> ➤ A BW-BEX report needs to be accessed from SAP BW and make it as data source for SAP BusinessObjects Analysis report. • SAP BusinessObjects Analysis report need to be created, formatted using excel add-in and then be saved into a server folder.
Report Users	<ul style="list-style-type: none"> ➤ Use the reports from SAP BusinessObjects Analysis for excel 	<ul style="list-style-type: none"> ➤ Copy Report from the application folder in BusinessObjects into own

		personal folder and execute reports for one or more application areas.
Power Users	<ul style="list-style-type: none"> ➤ Develop & Execute reports in SAP BusinessObjects Analysis for excel. 	<ul style="list-style-type: none"> ➤ Execute reports from one or more application areas directly from the application folders in Business Objects. ➤ Schedule report ➤ Create other SAP Business Objects Analysis reports.

1.2 Broad Category of Tasks in Business Objects Analysis

Tasks	Controlled by Authorization
SAP BW Report Development & Sourcing from Business Objects platform.	Controlled by SAP BW Authorization/Role Assignment
SAP Business Object Analysis for Excel Report Development, Execution & Scheduling.	Controlled by SAP BusinessObjects Authorization Assignment

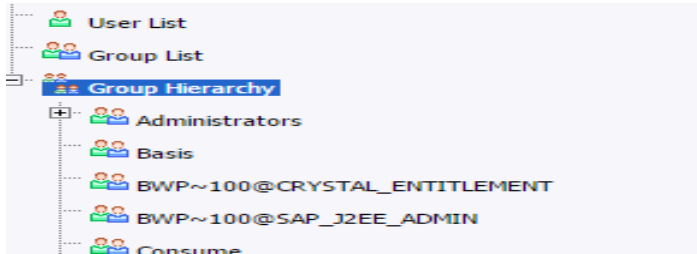
1.3 BW Authorization

BW Functional Roles		Role Assignment
Single role	Role name	<ol style="list-style-type: none"> 1. We have created different roles in SAP BW for different application areas (Such as FI, SD, MM etc). 2. Chosen BW-BEX reports from the specific application areas can be saved to the relevant roles, if we want to restrict the users in Business Objects to have restricted access. 3. Depending on the job-profile and the department they belong, roles are going to be assigned to BW business users and developers.
ZBW_ACCOUNTS_RECEIVABLE_EXEC_T	Accounts Receivable Query	
ZBW_CUSTOMER_SERV_QUERY_EXEC_T	Customer Service Query	
ZBW_FICO_QUERY_EXEC_T	FICO Query	
ZBW_FSCM_QUERY_EXEC_T	Dispute Management Query	
ZBW_MM_QUERY_EXEC_T	Materials Management Query	
ZBW_PLANT_MAINTENANCE_EXEC_T	Plant Maintenance Query	
ZBW_PROCUREMENT_QUERY_EXEC_T	Procurement Query	
ZBW_SD_QUERY_EXEC_T	SD Query	
ZBW_SUPPLY_CHAIN_EXEC_T	Suply Chain Query	
Composite role	Role name	
ZBWC_ACCTS_RECEIVABLE_EUSR_TST	Accounts Receivable End User	
ZBWC_CUSTOMER_SERVICE_EUSR_TST	Customer Service End User	
ZBWC_FICO_EUSR_TST	FICO End User	
ZBWC_FSCM_EUSR_TST	Dispute Management End User	
ZBWC_MM_EUSR_TST	BW MM End User	
ZBWC_PLANT_MAINTENANC_EUSR_TST	Plant Maintenance End User	
ZBWC_PROCUREMENT_EUSR_TST	Procurement End User	
ZBWC_SD_EUSR_TST	Sales & Distribution End User	
ZBWC_SUPPLY_CHAIN_EUSR_TST	Supply Chain End User	









Note: BW Authorization set up is covered in detailed, in appendix section below.

4. If Business Object users need to have different reporting access in Business Objects Analysis; in comparison to SAP BW users; then a new set of roles can be developed in SAP BW for SAP BusinessObjects environment. Through these new set of roles, same users can be allowed different report access in BO systems to BW reports.

1.4 Business Objects Authorization

BusinessObjects Access	Role Assignment																														
<p>User & Groups</p>  <p> <input type="button" value="Add Principals"/> <input type="button" value="Remove"/> <input type="button" value="View Security"/> <input type="button" value="Assign Security"/> </p> <table border="1"> <thead> <tr> <th></th> <th>Name</th> <th>Full Name</th> <th>Type</th> <th>Access</th> </tr> </thead> <tbody> <tr> <td></td> <td>Administrators</td> <td></td> <td>User Group</td> <td>Full Control (Inherited)</td> </tr> <tr> <td></td> <td>Basis</td> <td></td> <td>User Group</td> <td>Full Control (Owner)</td> </tr> <tr> <td></td> <td>Developers</td> <td></td> <td>User Group</td> <td>Full Control (Owner)</td> </tr> <tr> <td></td> <td>End Users</td> <td></td> <td>User Group</td> <td>Advanced (Inherited)</td> </tr> <tr> <td></td> <td>Everyone</td> <td></td> <td>User Group</td> <td>No Access</td> </tr> </tbody> </table> <p>Folders</p> <ul style="list-style-type: none"> Accounts Receivable Customer Service Finance & Controlling Materials Management Materials Management Sales & Distribution Supply Chain Management Procurement Financial Supply Chain Management 		Name	Full Name	Type	Access		Administrators		User Group	Full Control (Inherited)		Basis		User Group	Full Control (Owner)		Developers		User Group	Full Control (Owner)		End Users		User Group	Advanced (Inherited)		Everyone		User Group	No Access	<ol style="list-style-type: none"> 1. Import "Roles" & "Users" from SAP BW. 2. Create various "User groups" in SAP Business Objects CMC platform such as "Developer" or "Administrator" or "Report Users" or "Power Users – Finance", "Power Users – Operation", "Power Users – Procurement", "Power Users – CS", "Power Users – SC", "Power Users – AR" etc. 3. Assign the imported "Roles" to various "User Groups" created in Step 2. Right click on the imported roles → choose "Join Group" → Choose the groups listed above one by one. 4. Create various "Folders" in CMC, for report management of different application areas; such as "Finance", "Procurement", "Operations", "Customer Service", "Supply Chain" & "Accounts Receivable" etc.
	Name	Full Name	Type	Access																											
	Administrators		User Group	Full Control (Inherited)																											
	Basis		User Group	Full Control (Owner)																											
	Developers		User Group	Full Control (Owner)																											
	End Users		User Group	Advanced (Inherited)																											
	Everyone		User Group	No Access																											

Access Level

	Name ^
	Demo level
	Full Control
	Full Control (Owner)
	Schedule
	Testing
	View
	View On Demand
	ZSchedule

5. When we create any new “Folder”, three sets of permissions are automatically assigned: Administrator, Developer and Everyone. “Administrators” are given the access level “Full Control”. “Everyone” is given the access level “No Access”. “Developers” are given the access level “Full Control”.
6. Select each Folder → Right click → User Security → Add Principles → Select Groups. **Each folder should have “Administrators”, “Developers”, “Everyone”** mandatorily. In addition, they should have the application specific groups. **For example:** the FINANCE Folder should have following groups; “Power user – Finance” & “Report user – Finance”, in addition to “Administrator”, “Developer” & “Everyone”. Once a **Principal / Group** are assigned to a folder, we can choose → “Add/Assign Security”.
7. At this stage, we will be required to choose either “**Generic Access levels**” such as “Full control”, “Schedule”, “View” or “View on demand” **or** we can create custom access level **or** we can even maintain “**ADVANCED access level**” analysing complex scenario with set of very detailed parameters from “**Advance**” tab.
 - Access Levels need to be defined for each of the User or User Groups assigned to the folders.
 - “Grant” radio button can be selected for providing various accesses such as to schedule a report, view, Pause and

	<p>resume its Scheduled instances etc.</p> <ul style="list-style-type: none"> • “Deny” radio button can be selected to deny access to other activities such as accessing any folder or report, and to view, delete a report. • We can also allow the rights to be applied to a “Sub object”, by checking the Object and Sub Object check boxes, next to the Rights column. • Only after we click grant or deny radio button, “Object” and “Sub-object” check boxes are enabled. Now we can maintain the scope of rights. • If we want to apply a right only for a “Folder” and “not for its “Sub folders”, then we can uncheck sub-object check box.
--	--

Note: Unlike SAP systems, Business Object Enterprise do not comprise of Roles, Profiles and Authorization objects. Security in Business Objects is different than SAP and it consists of: Folder level security, Application Security, Object Level Security and inheritance concepts.

1.4.1 Assignment of User Groups & Roles to the Folders in Business Objects in CMC

Business Object Server Folders	User Group Assignment to the Folders	BW Role Assignment to the Group
Finance & Controlling	<ul style="list-style-type: none"> • Developer • Administrator • Everyone • Power user – Finance • Report user – Finance 	Role from SAP BW Containing all the Finance specific reports we want to be accessible in BO Analysis for excel.
Procurement	<ul style="list-style-type: none"> • Developer • Administrator • Everyone • Power user – Procurement • Report user – Procurement 	Role from SAP BW Containing all the Procurement specific reports we want to be accessible in BO Analysis for excel.
Financial Supply Chain Management	<ul style="list-style-type: none"> • Developer • Administrator • Everyone • Power user – Operations • Report user – Operations 	Role from SAP BW Containing all the FSCM specific reports we want to be accessible in BO Analysis for excel.
Customer Services	<ul style="list-style-type: none"> • Developer • Administrator 	Role from SAP BW Containing all the Customer Services specific reports we want to be accessible

	<ul style="list-style-type: none"> • Everyone • Power user – Customer Services • Report user – Customer Services 	in BO Analysis for excel.
Supply Chain Management	<ul style="list-style-type: none"> • Developer • Administrator • Everyone • Power user – Supply Chain • Report user – Supply Chain 	Role from SAP BW Containing all the Supply Chain specific reports we want to be accessible in BO Analysis for excel.
Accounts Receivable	<ul style="list-style-type: none"> • Developer • Administrator • Everyone • Power user – Accounts Receivable • Report user – Accounts Receivable 	Role from SAP BW Containing all the Accounts Receivable specific reports we want to be accessible in BO Analysis for excel.
Plant Maintenance	<ul style="list-style-type: none"> • Developer • Administrator • Everyone • Power user – Plant Maintenance • Report user – Plant Maintenance 	Role from SAP BW Containing all the Plant Maintenance specific reports we want to be accessible in BO Analysis for excel.
Sales & Distribution	<ul style="list-style-type: none"> • Developer • Administrator • Everyone • Power user – Sales & Distribution • Report user – Sales & Distribution 	Role from SAP BW Containing all the Sales & Distribution specific reports we want to be accessible in BO Analysis for excel.
Materials Management	<ul style="list-style-type: none"> • Developer • Administrator • Everyone • Power user – Materials Management • Report user – Materials Management 	Role from SAP BW Containing all the Materials Management specific reports we want to be accessible in BO Analysis for excel.

1.4.2 Relationship between Access Levels and User Groups in Business Objects CMC

Access Level	Rights	User Groups
No Access	The no access level may be misleading. The no access level does not explicitly deny access, but rather, sets all permissions to “Not Specified.” This can be overridden through inheritance.	Everyone
View	<p>When set at the folder level, the user can view the folder, the objects contained in the folder, and all generated instances of each object.</p> <p>At object level, the user can view the object, history of the object, and all generated instances of the object.</p> <p>The user cannot schedule or refresh the report, however by default; the user can edit the report and save to a personal folder to refresh there. We can deny users from copying the object by going to advanced and denying</p>	Occasional Users / Report Users

	“Copy Objects to another folder”	
Schedule	A user can generate instances by scheduling the object to run against a specified data source once or on a recurring basis. The user has full access to the scheduled instances that they own. They can also schedule to different formats and destinations, set parameters, pick servers to process jobs, add contents to the folder, and copy the object or folder.	Developers Administrators Power-Users
View On Demand	A user can refresh a report in real time. Note that if a report is a WEBI document, the user will also need View On Demand access to the universe and universe connection to perform the refresh.	Power Users
Full Control	Allows users to modify all of the object’s properties. This is the only access level that allows users to delete objects.	Developers Administrators

2 Authorization Strategy

Model – Separating Functional Access Groups from Data Access Groups

- This model is probably the most common model to implement as it has the right balance between flexibility and cost of development and maintenance. **Here we have 2 sets of groups: one that defines “functional access” and one that defines “application access”. A user is then a member of one of the functional groups and one or more application groups; this then defines overall access strategy.**

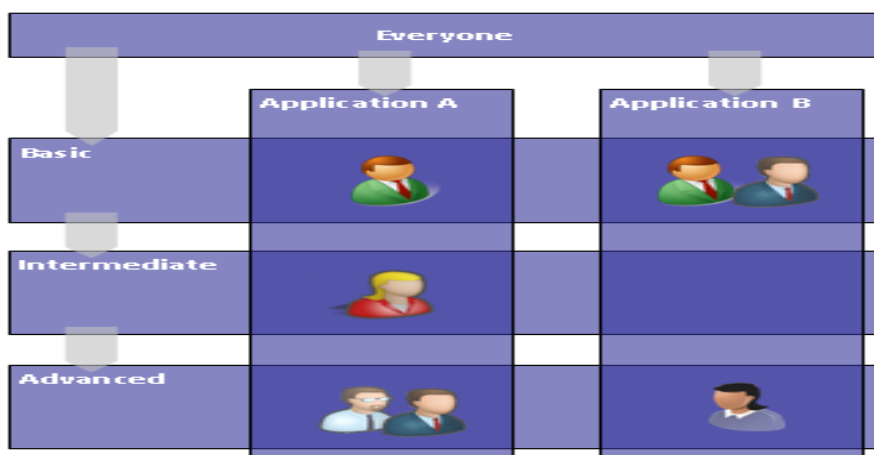
Functional Groups

- We first define the required functional access groups. We can have 3 functional groups of “Basic” (Report Users), “Intermediate” (Power Users) and “Advanced” (Developer or Administrators); where again we have an inheritance model of increasing rights. This, along with the “Everyone” group defines the ‘baseline’ security model. Users will be a member of at most one of these 3 groups, if a user is in more than one then the resolved access will be that of the more advanced group.

BI Application Groups

- We also create user groups that define separate BI Applications. The BI application (FI, FI-AP, FI-AR, SD, MM, PUR etc) itself defines data access, that is, it controls access to reports and universes that comprise the application. Users can belong in one or more of these groups.

A user then belongs to one functional group and one or more application groups. It should be noted that a user can then only have the same functional access across applications. I.e. if a user is a “Basic” user in one application they must also be a Basic user in any other application they have access to. A second similar point is that each application must reuse same functional access model, that is, we can’t have two Basic groups with different functional access in two different applications.



Proposed Access Level & Data Access Profile of Various user types:

Access Level	User Types	FI	CS	AR	SD	MM	PM	SCM	FSCM	Procurement
View	Report Users	X	X	X	X	X	X	X	X	X
View	Report Users - FI	X								
View	Report Users - SD				X					
View	Report Users - MM					X				
View	Report Users -F SCM								X	
View	Report Users - SCM							X		

View	Report Users -AR			X						
View	Report Users - CS		X							
View	Report Users - PR									X
View	Report Users - PM						X			
View on Demand	Power Users	X	X	X	X	X	X	X	X	X
View on Demand	Power Users - FI	X								
View on Demand	Power Users - SD				X					
View on Demand	Power Users - MM					X				
View on Demand	Power Users - FSCM								X	
View on Demand	Power Users - SCM							X		
View on Demand	Power Users -AR			X						
View on Demand	Power Users - CS		X							
View on Demand	Power Users - PR									X
View on Demand	Power Users - PM						X			
Full Access	Developer	X	X	X	X	X	X	X	X	X
Full Access	Administrator	X	X	X	X	X	X	X	X	X

3 Step-by-Step SAP BusinessObjects Authorization Configuration

This document covers how to create users, user groups and ends with creating access Levels and basic troubleshooting techniques using the Security Query.

3.1 User and User Group Creation:


Users in Business Objects can be of various types, and a user can login to Business Objects using that particular authentication with which the user has been created with. The authentications are:

1. Enterprise
2. LDAP
3. Windows AD
4. SAP

In our context; "SAP" user authentication is appropriate and users are created with.

3.2 STEP 1: Creating a User:

The example below illustrates "How to create a user" in Business Objects.

Login to **CMC** → Go to **Users and Groups**, by selecting appropriate icon  from left hand side bar.

To create a new **User** click on  and for **User group** creation click on 
OR

Click **Manage**:



Select the Authentication Type in the next screen and maintain the required fields.

1) Authentication Type as **SAP** :

- When Authentication type is **SAP**, then we only need to maintain Account Name as **<SAP SID>~<Client No.>/<SAP User ID>** .
- User will login in Business Object Using his SAP Login credentials.

- **Connection Type:**
 - **Concurrent** : This user belongs to a license agreement that states the number of users allowed to be connected at one time.
 - **Named** : This user belongs to a license agreement that associates a specific user with a license. Named user licenses are useful for people who require access to Business Objects Enterprise regardless of the number of other people who are currently connected.

Click **Create & Close**

NOTE: “Administrator” is the default user that comes along with the Business Objects installation.

3.3 STEP 2: User Group Creation

The user group is a collection of users who require same kind of authorization. So instead of assigning authorization to every new user that is created, we can create a user group and assign the requisite authorization to it, and later simply assign the user to that particular user Group.



Click **Create User group:**

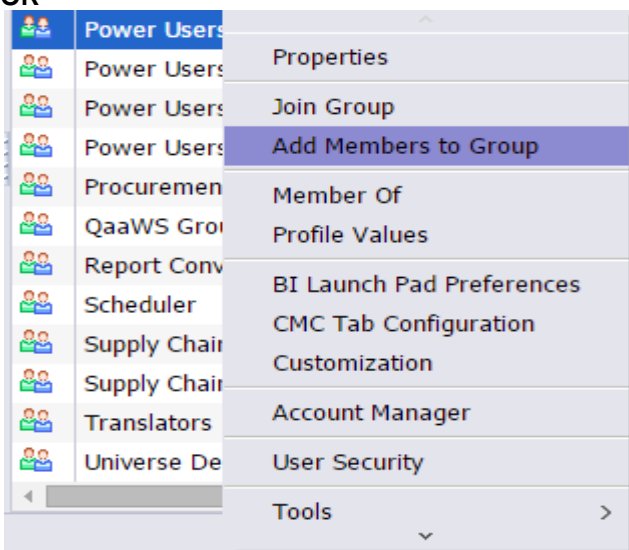
Name the User Group:

Click “OK”.

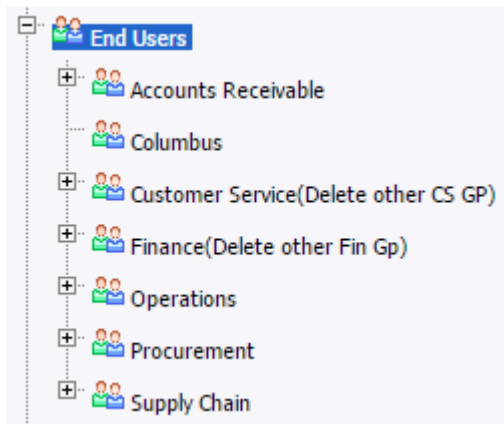
Once a User Group is created, we can add a user to the group click (**Add member to user group**); by selecting the below icon from the MENU BAR.



OR



We can add a newly created or existing group to some other group while we can also assign a user to a group. All the BW roles, once imported to BO CMC appear as User Groups as well. This is because they are already assigned to users from BW based on their configuration in BW. We can assign these roles (which appear as User Groups in BO CMC) to the newly created User Groups.



NOTE: Administrators and Everyone are the default groups that come along with the Business Objects installation.

3.4 STEP 3: Importing Roles from the backend SAP BW system

This section covers 'How to import roles', which in turn import users from a backend SAP BW system to the Business Objects System.

Manage

Authentication ▼

- Instance Manager
- Applications
- Settings
- Sessions
- Authentication

Type	Title
	Enterprise
	LDAP
	SAP
	Windows AD

Entitlement Systems

Entitlement Systems

Role Import

SNC Settings

Options

User Update

Logical system name

System Client

Disabled

Load balancing

Message Server

Logon Group

Application host

Application Server

System Number

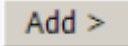
User name

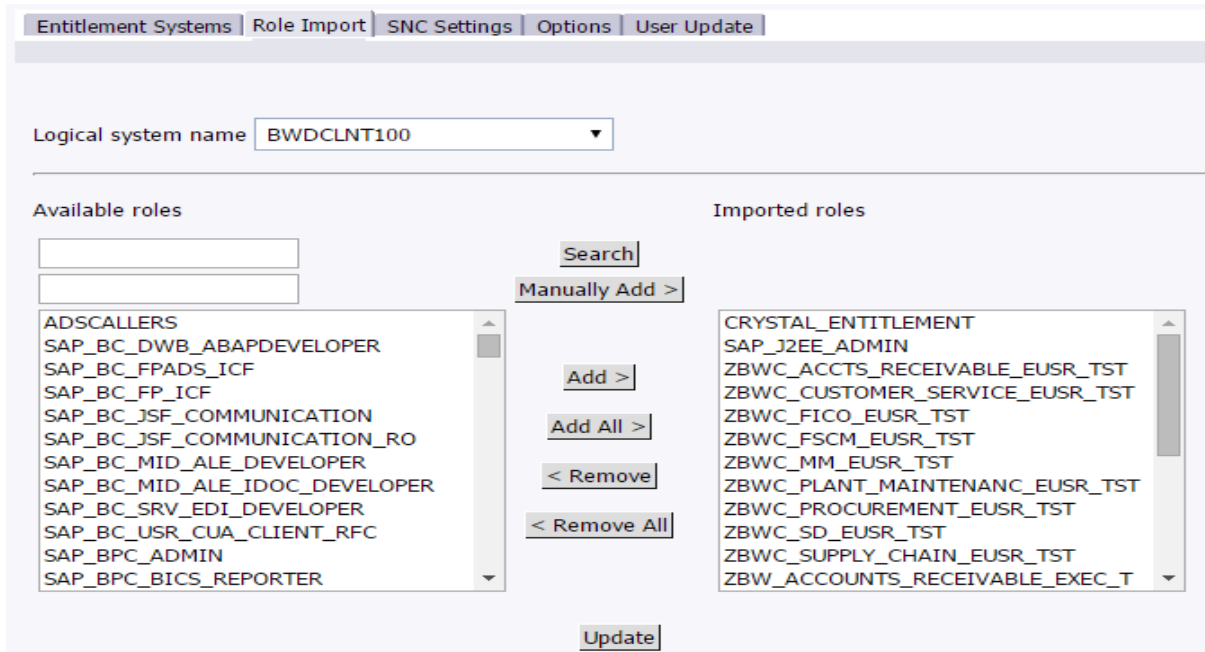
Password

Language

Login to the **CMC** → Click **Authentication** → **SAP**

Since our Business Objects System is connected to a Backend SAP BW System; we are able to see a list of Roles in the left Pane which belong to the SAP BW system. We can now Import the roles from the Backend SAP BW system to the Business Objects system, select the role in the left pane and

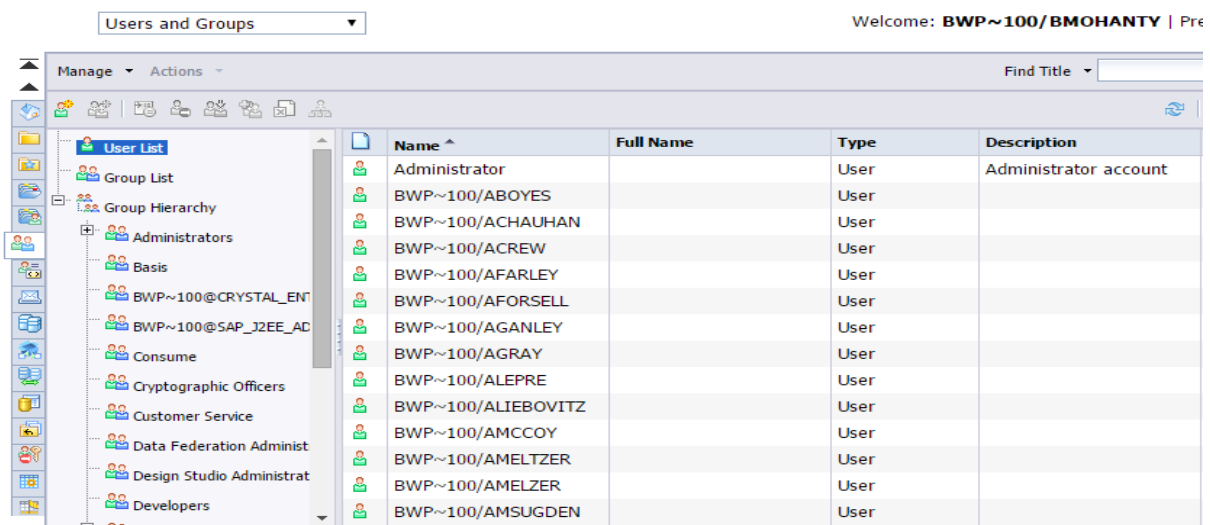
click  to import the roles then click **Update:**



When a role is imported all the users assigned to that role in our backend SAP BW system, will also get imported into the Business Objects system.

Now when a new user get assigned to an existing role in backend in SAP BW, only we need to click **Update Now** button under **User Update** tab and the user will get created in the Business Objects system. To automate this activity also, we have already elaborated the steps in the next sections.

Central Management Console



Here, BWP is our SAP system Id, while 100 is the client number from where the users arrive, hence the naming convention: **BWP~100/**.

3.5 STEP 4a: Automating Importing of Roles from SAP BW system into Business Objects

Click the **User Update** tab, now we need to check the field **“Update now”** or **“Schedule”** to import the **“Role”** or **“Role and Alliances”** information from SAP BW.

Whenever a user assignment is done to a role in backend (which has already imported in Business Objects) and user should get created in Business Objects. To create/update them automatically we should use **Schedule** button. We can also force Synchronization under **User Update** tab by clicking **Update Now** button.

User Update

Entitlement Systems | Role Import | SNC Settings | Options | **User Update**

Manage regular updates of user roles only or of user roles and user aliases from SAP systems. Run the update once by selecting "Update Now," or set up a regularly scheduled update.

Update Roles Only

Update Now | Schedule... | Cancel Scheduled Updates

Last Scheduled Update: There is no record of a previous update attempt.
Next Scheduled Update: Roles update has not been scheduled.

Update Roles and Aliases

Update Now | Schedule... | Cancel Scheduled Updates

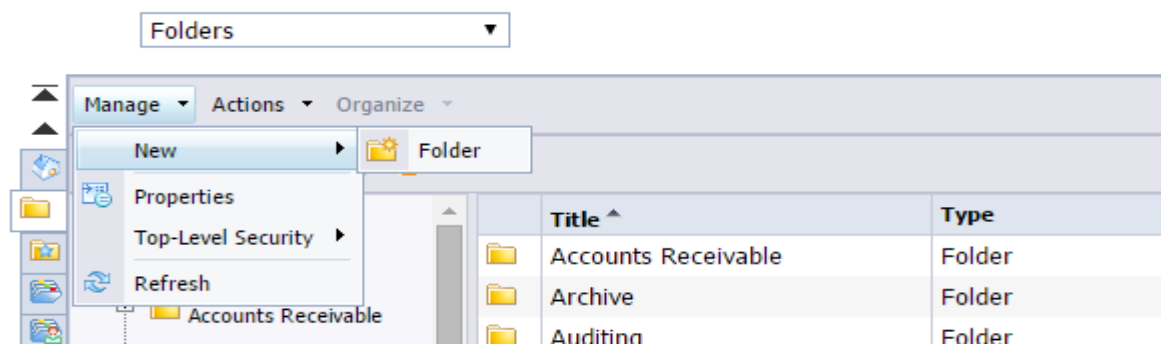
Last Scheduled Update: There is no record of a previous update attempt.
Next Scheduled Update: User alias update (including roles) has not been scheduled.

3.6 STEP 4b: Schedule a SAP Authentication Role update in Business Objects using a java program

To schedule (automate) the updating of SAP Users in the Business Objects system, we need to follow the steps mentioned below:

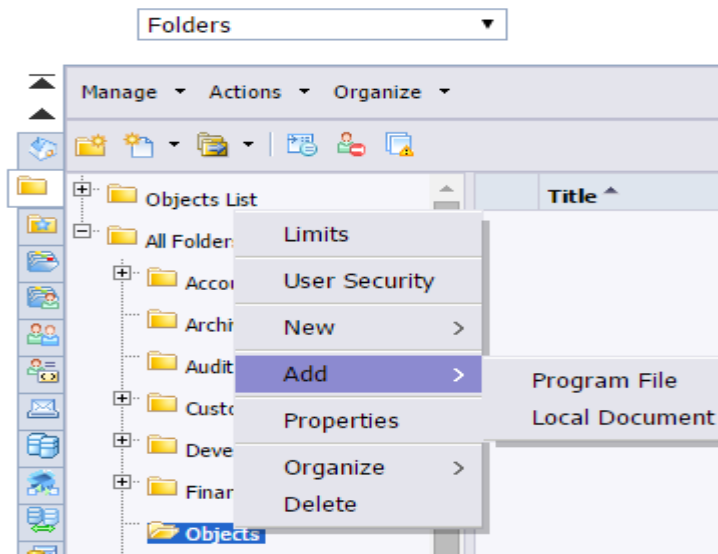
1. Download **SAP Update.jar** file from SAP Note: 1406037
2. Unzip the file
3. Login in Business Objects **CMC** → **Folders** → **Manage** → **New** → **Folder** → name **“Objects”**

Central Management Console



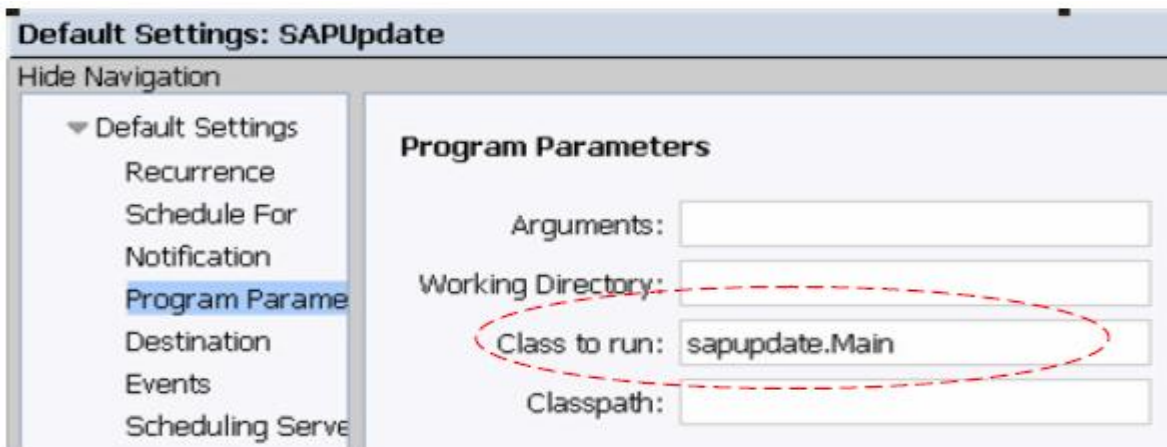
4. Select the folder **“Objects”** and click on **Manage | Add | Program File**

Central Management Console

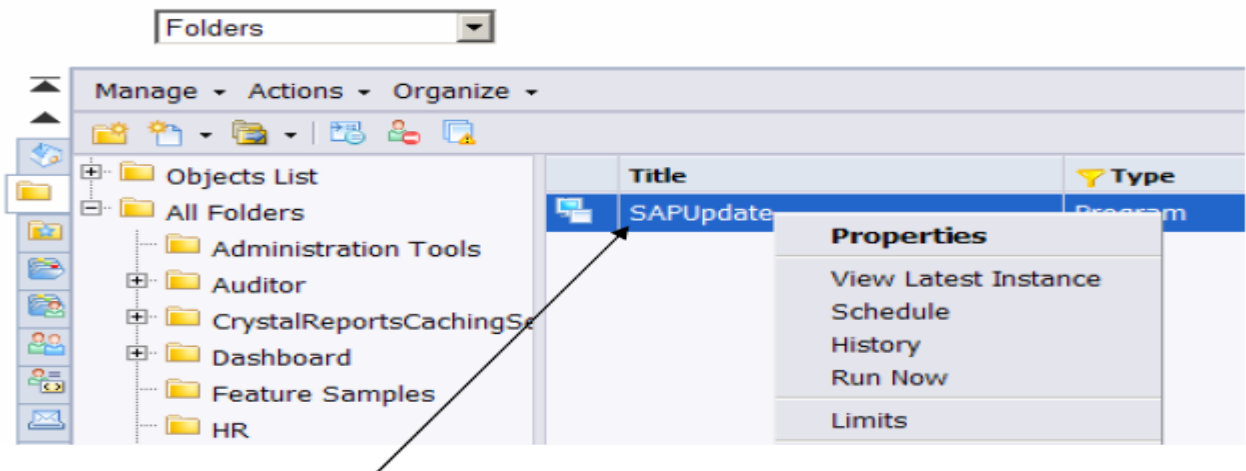


5. Choose as Program Type as **Java** and add **SAPUpdate.jar** from the local drive.

6. Right Click on SAPUpdate within our **Objects** folder and choose → **Properties** → **Default Settings** → **Program** → **Parameters** → Specify as "Class to run:" sapupdate.Main



Use the **"Run Now"** or **Schedule** the Program Object. Recurrence for this Program can be set as desired.



Now, the SAP BW users will get imported every time when they are created and assigned to a role in the SAP BW system which has already been imported in Business Objects CMC. As such, there is no

need to create a user in the Business Object CMC every time a new user is created in the SAP BW system. .

Note: The statement assumes that every user which is created in the SAP system needs to be created in Business Objects system. Else, if all the users are not required in the Business Objects system, the role which is imported in the Business Objects system should not be assigned to such users in the SAP backend. Two different roles can be created in that case, one for BW and one for Business Objects.

3.7 STEP 5: Standard Access Levels

Pre-Defined access levels:

There are four default access levels that come along with the Business Objects Installation for securing the content. These levels are explained as below:

1. **Full Control:** A principal has full administrative control of the object.
2. **Schedule:** A principal can generate instances by scheduling an object to run against a specified data source once or on a recurring basis.
3. **View:** If set on the folder level, a principal can view the folder, View objects within the folder, and each object's generated instances.
4. **View on Demand:** A principal can refresh data on demand against a data source.
5. **No Access:** The user or group is not able to access the object or folder.

Central Management Console

Name	Description	Date Modified
Full Control	Grants full access	Nov 2, 2014 1:11 AM
Full Control (Owner)	Grants owner version of all rights	Jan 30, 2014 11:32 AM
Schedule	Grants all rights from View, as well as rights to schedule objects	Nov 2, 2014 1:11 AM
Testing		Mar 26, 2014 10:17 AM
View	Grants view rights for objects	Nov 2, 2014 1:11 AM
View On Demand	Grants all rights from Schedule, as well as rights to refresh documents	Nov 2, 2014 1:11 AM
ZSchedule	Users with this access level can schedule but can't view the reports. To	Aug 12, 2014 2:17 PM

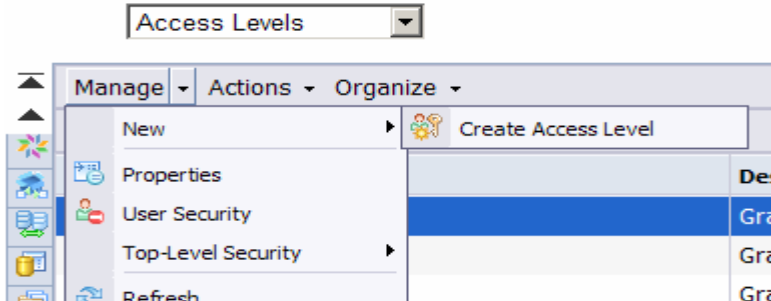
To see what rights are included in an access level; Go to **CMC** → select **Access Level** → Right click - > **Include rights**

Name	Description
Full Control	Grants full access
Full Control (Owner)	Grants owner version of all rights
Schedule	Grants all rights from View, as well as rights to schedule objects
Testing	
View	Grants view rights for objects
View On Demand	Grants all rights from Schedule, as well as rights to refresh documents
ZSchedule	Users with this access level can schedule but can't view the reports. To

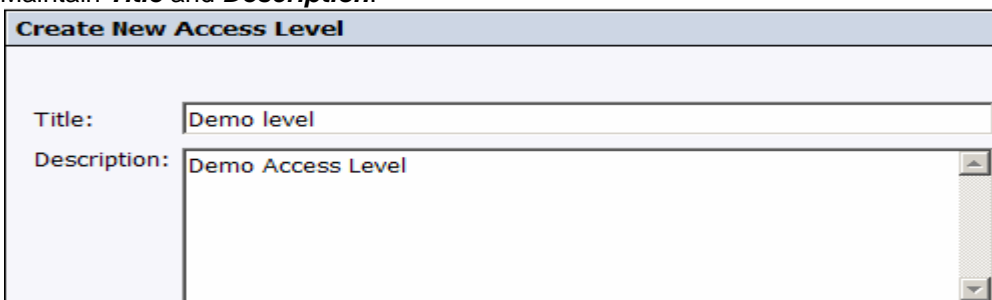
3.8 STEP 6: Custom Access Levels

In addition to the predefined access levels, we can also create and customize our own access level, which can greatly reduce administrative and maintenance costs associated with security.

To create access levels: Login to **CMC** → Select **Access Levels**.

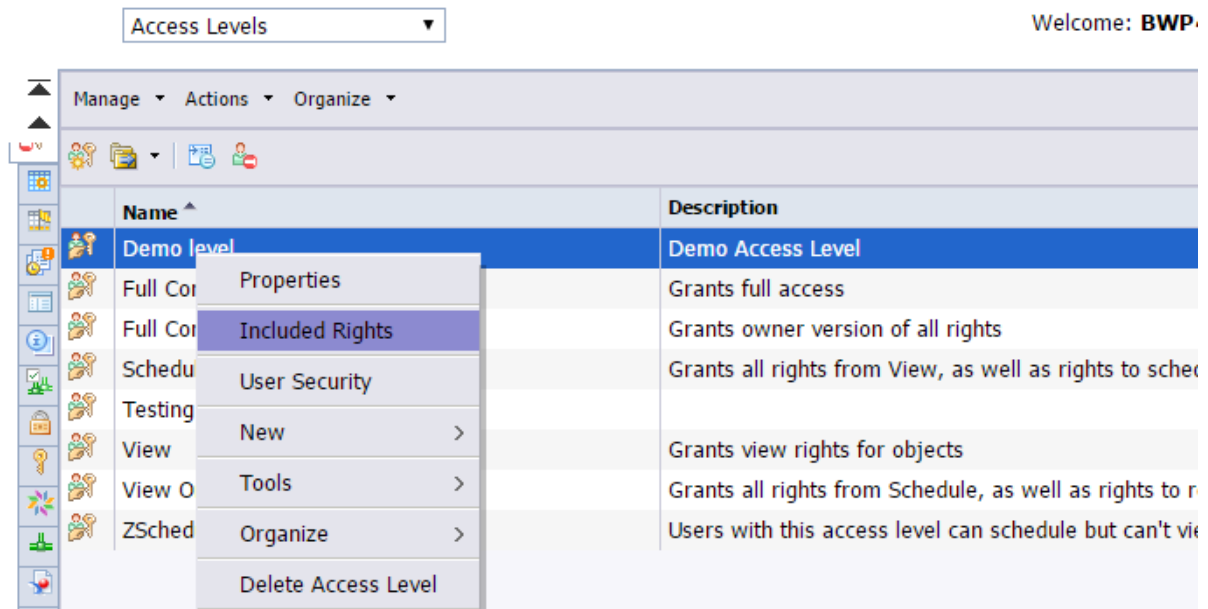


Maintain **Title** and **Description**:

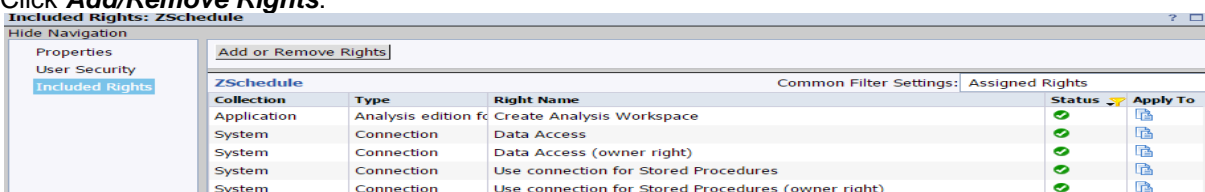


To include rights in an access level, select the **Access level**, right click -> **included rights**

Central Management Console



Click **Add/Remove Rights**:



We will be able to see four types of rights collections in the left panel namely:

- General
- Content
- Application
- System



By default we will be guided to the “**General Global rights**” window. Each “General global rights” can have a status of:

- Granted
- Denied
- Not Specified.
- Apply to the Object
- Apply to the Sub-Object

We can also choose whether to apply these rights to the object only or to their sub-objects only, or both. To set type-specific rights for the access level, in the navigation list, click the **Rights collection**, and then click the Sub collection that applies to the object type we want to set the rights for.

▼General Global Rights	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Add objects to folders that the user owns	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Add objects to the folder	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Change password for users that the user owns	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Change preferences	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Change preferences for objects that the user owns	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Change user password	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Comment on documents	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Comment on documents owned by the user	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Copy objects that the user owns to another folder	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Copy objects to another folder	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Define server groups to process jobs	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Define server groups to process jobs for objects that the user owns	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Delete instances	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Delete instances that the user owns	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

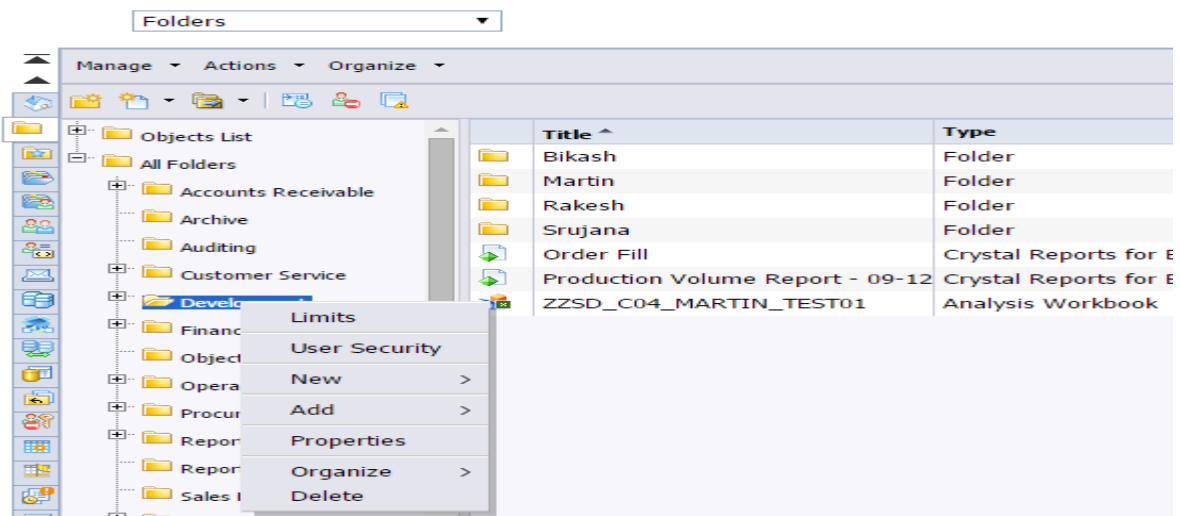
3.9 STEP 7: Folder level Security

Folder-level security enables us to set access-level rights for a folder and the objects contained within that folder. While folders inherit security from the top-level folder (root folder), subfolders inherit the security of their parent folder. Rights set explicitly at the folder level override inherited rights.

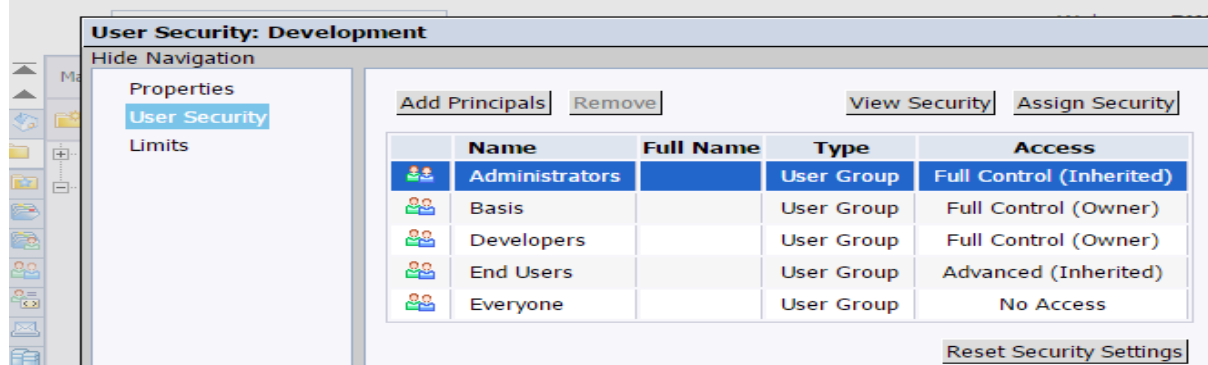
To set folder level security:

1. Login to **CMC** → Select **Folders**
2. Right click on the particular folder → select **User Security**.

Central Management Console



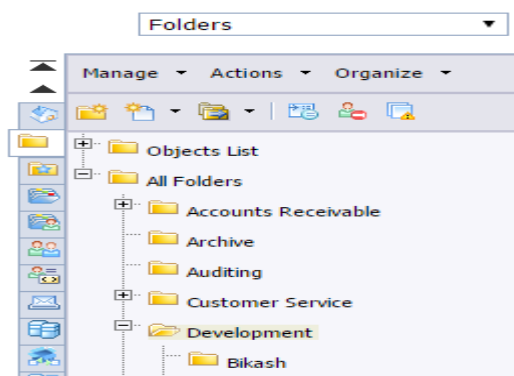
Central Management Console



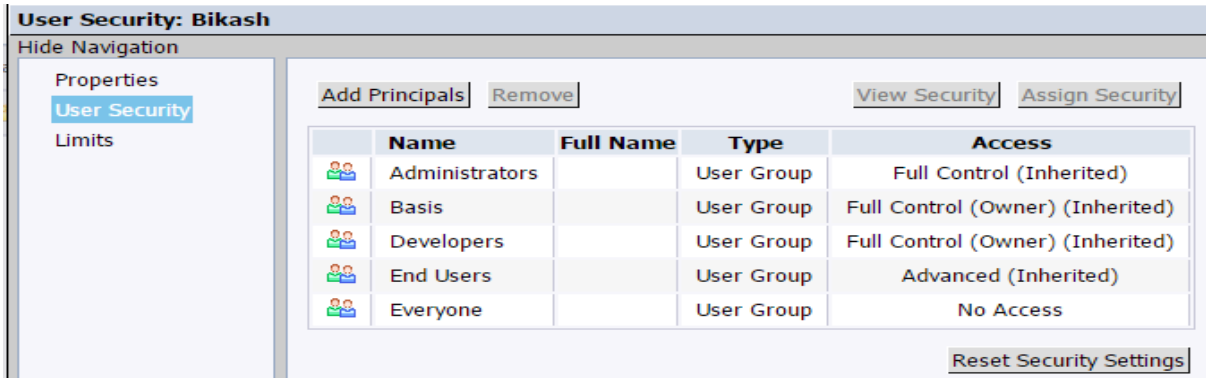
If we analyse the “Folder Level security” for “Development” folder, we can see following:

- “Administrators” have inherited “Full Control”
- “End Users” have inherited “Advanced” Access level.
- “Developers” have been given “Full Control”
- “Basis team members” have been given “Full Control”
- And “Everyone else” has “No Access”.

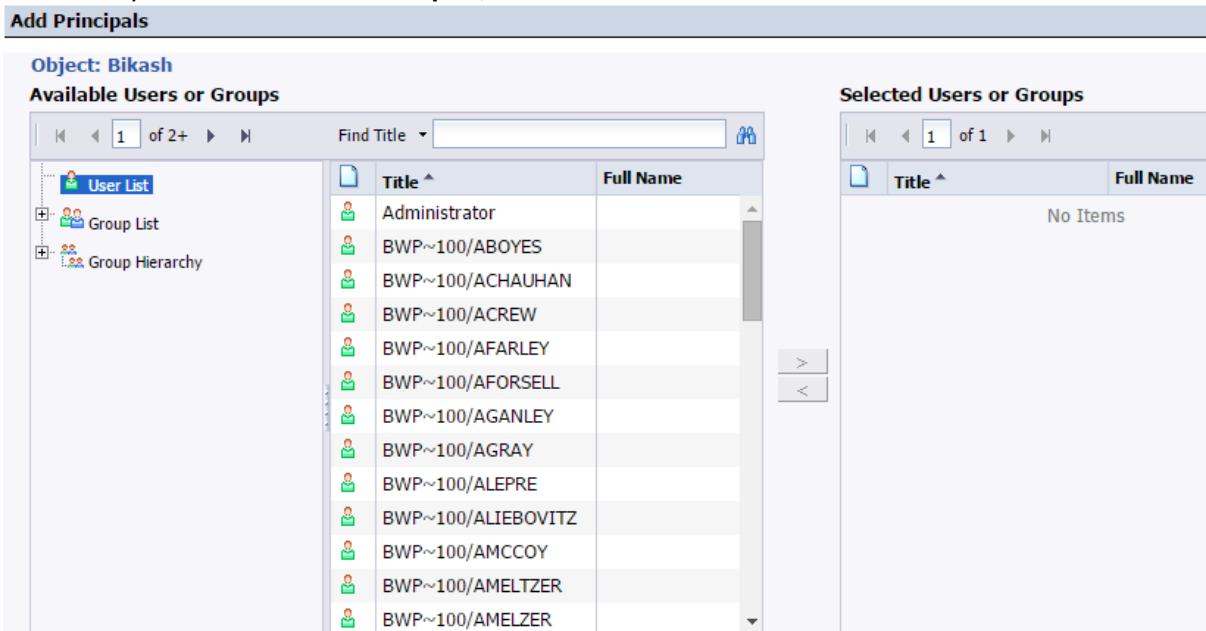
Central Management Console



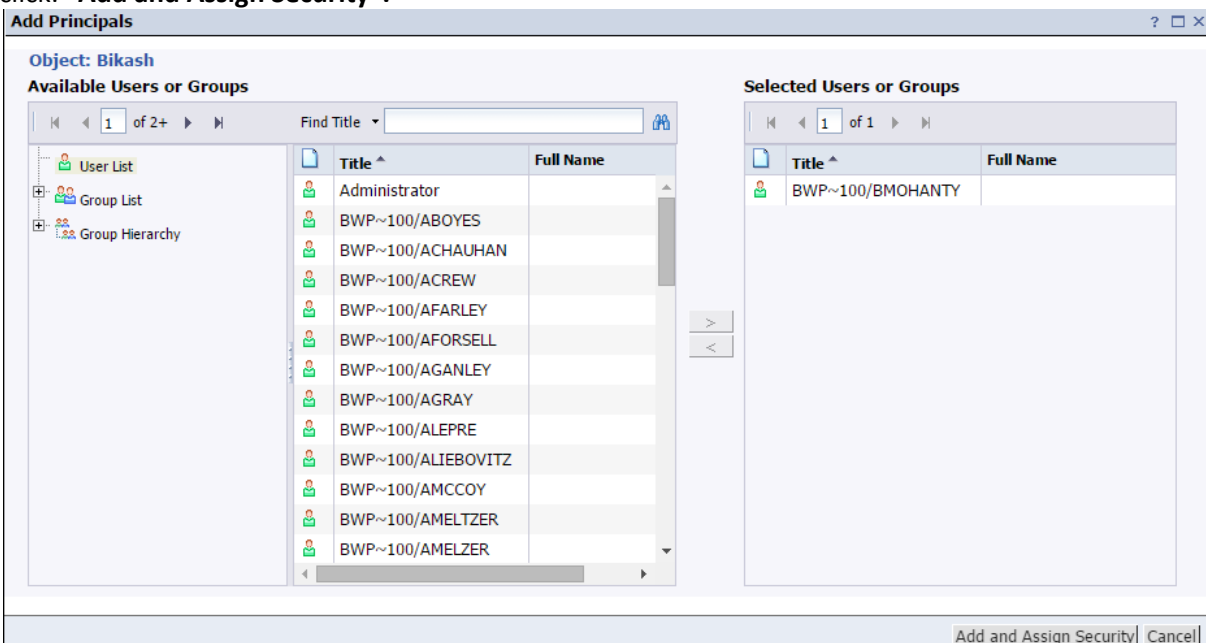
“Bikash” is a folder under “Development” folder. Hence everything inherited from the “Access Level” at the “Development” folder.



Additionally we can add other **Principals**, as well.

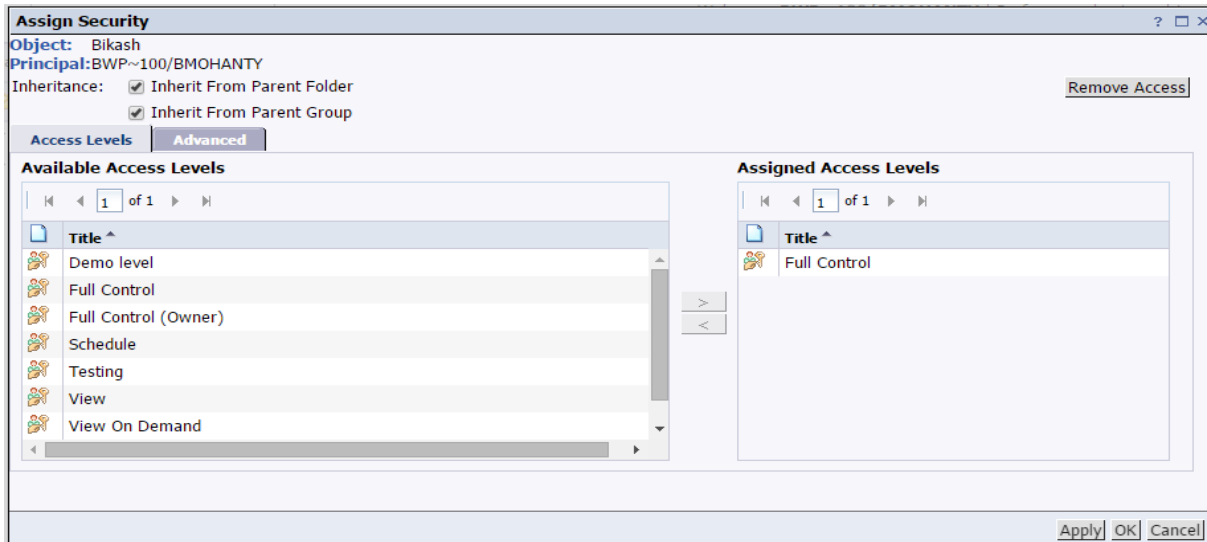


Select the **Principal** (user / group) we wish to add. On the same screen in the bottom right corner click: **“Add and Assign Security”**.

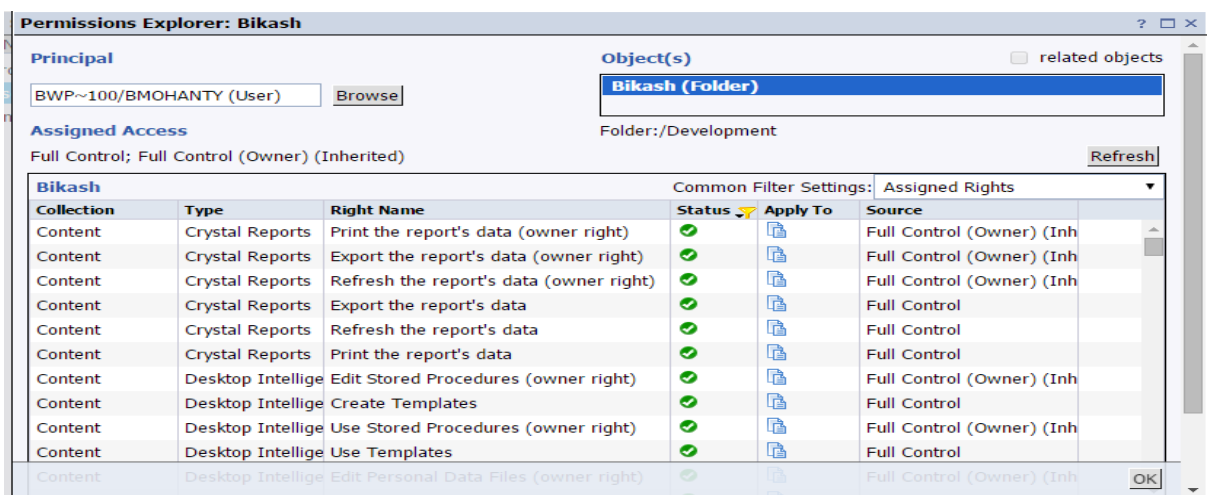
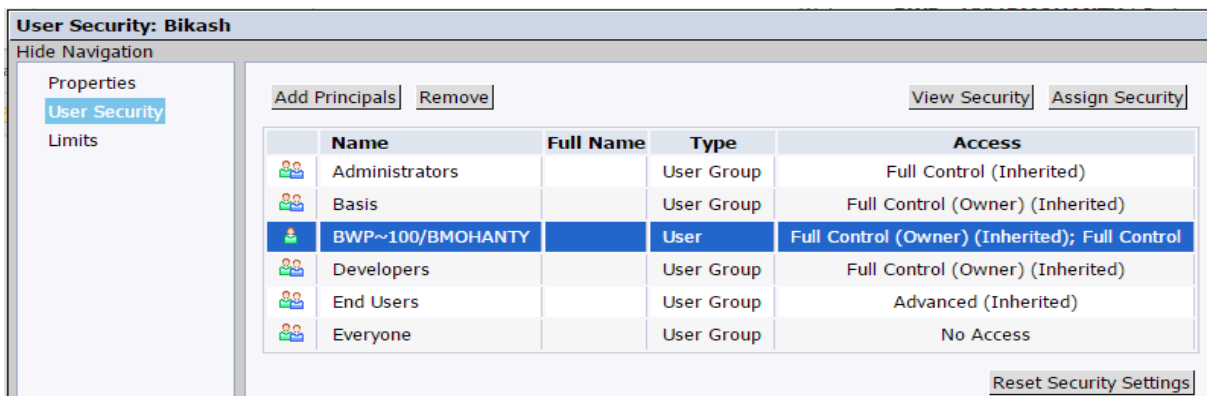


Assign the appropriate “Access Levels” and on the same screen in the bottom right corner click: “Apply” and “OK”.

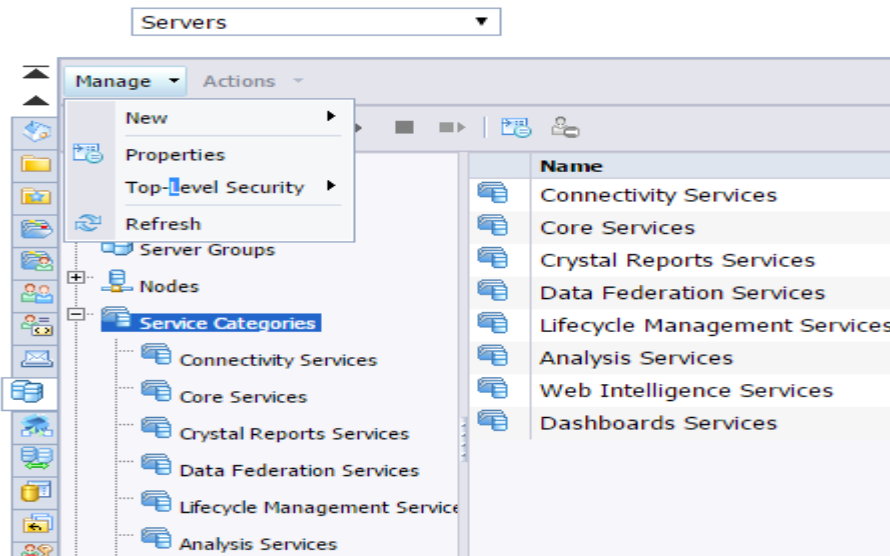
To provide the requisite “Full Control”; Access Level to this Principal “BMOHANTY”. Here is what we do. Click **Apply**, and then Click **OK**.



To View, what access has been provided to the Principal click “View Security”

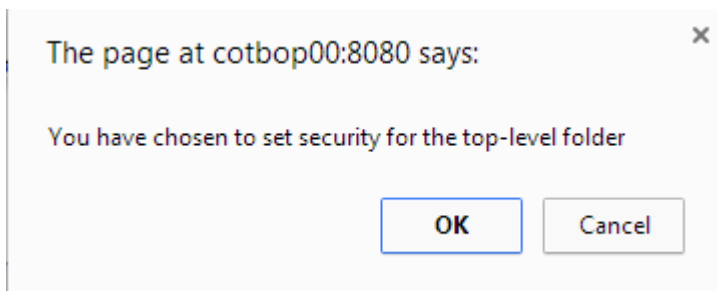


4 Top Level / Server Level Security: Central Management Console

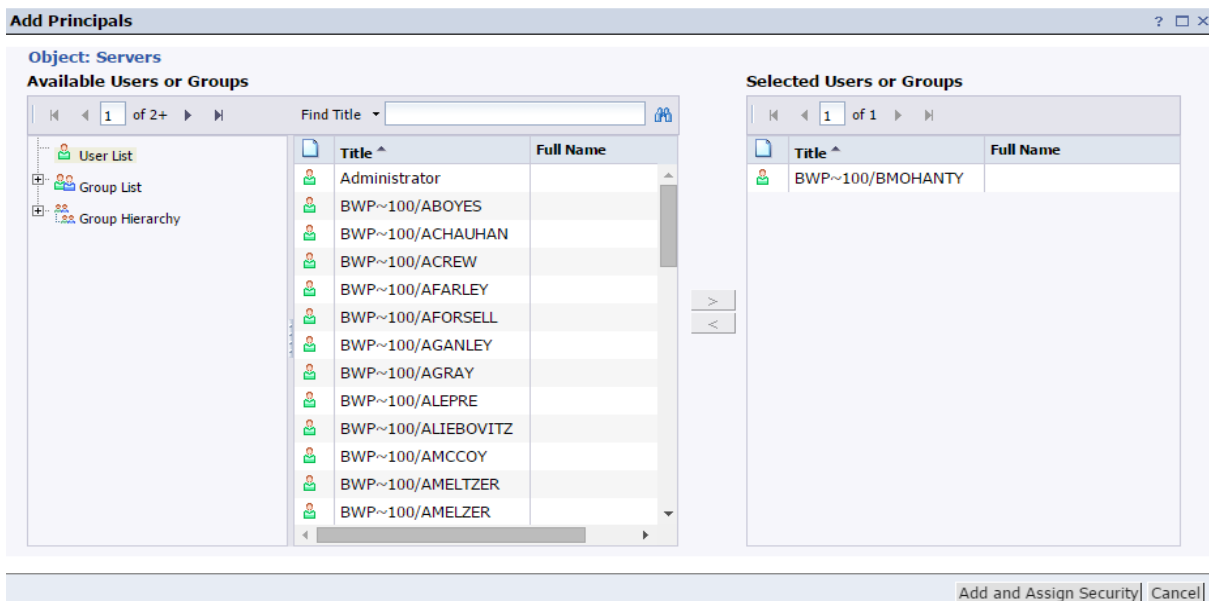


This example shows, how Top Level Security can be assigned to a principal against the Business Objects Servers: [Manage the Top Level Security for Servers](#): For this:

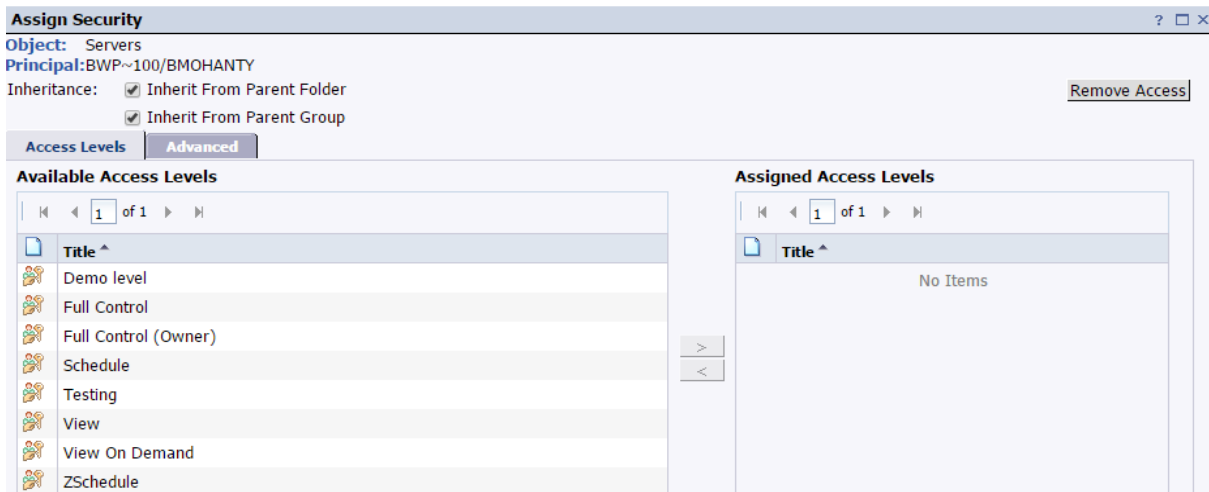
1. Login to **CMC** -> **Servers**-> **Manage**
2. Select **Top Level Security** _ **All Servers** ➔ **All Server Groups**.



Click OK.



Add Principals

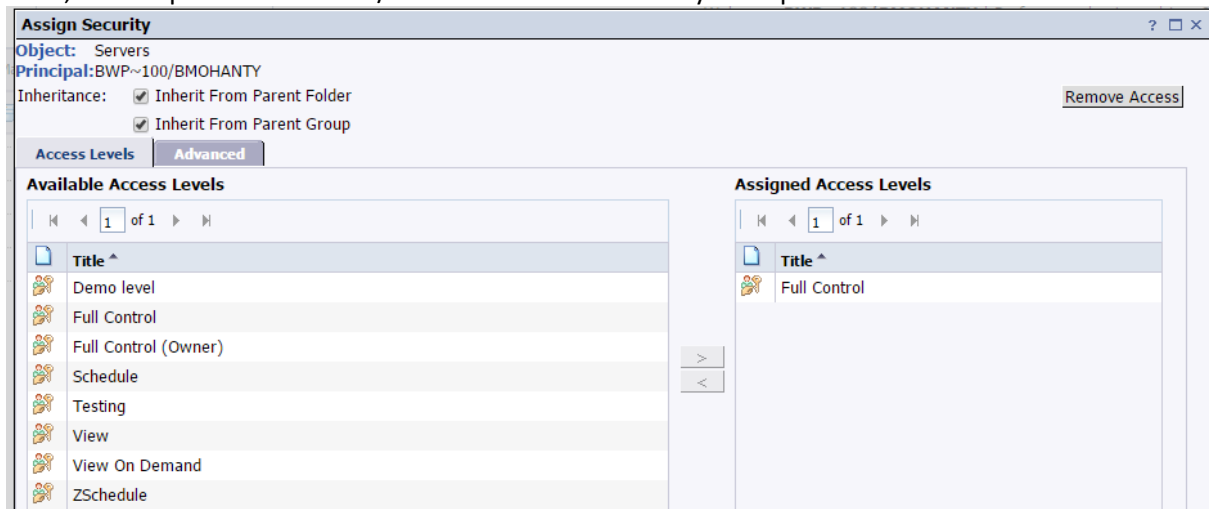


To Break Inheritance:

If our Principal is a part of multiple groups and to avoid “Conflict of Rights” we can uncheck the:

1. Inherit From Parent Folder
2. Inherit From Parent Group.

Now, we can provide “Access” / “Advanced level” security as required.

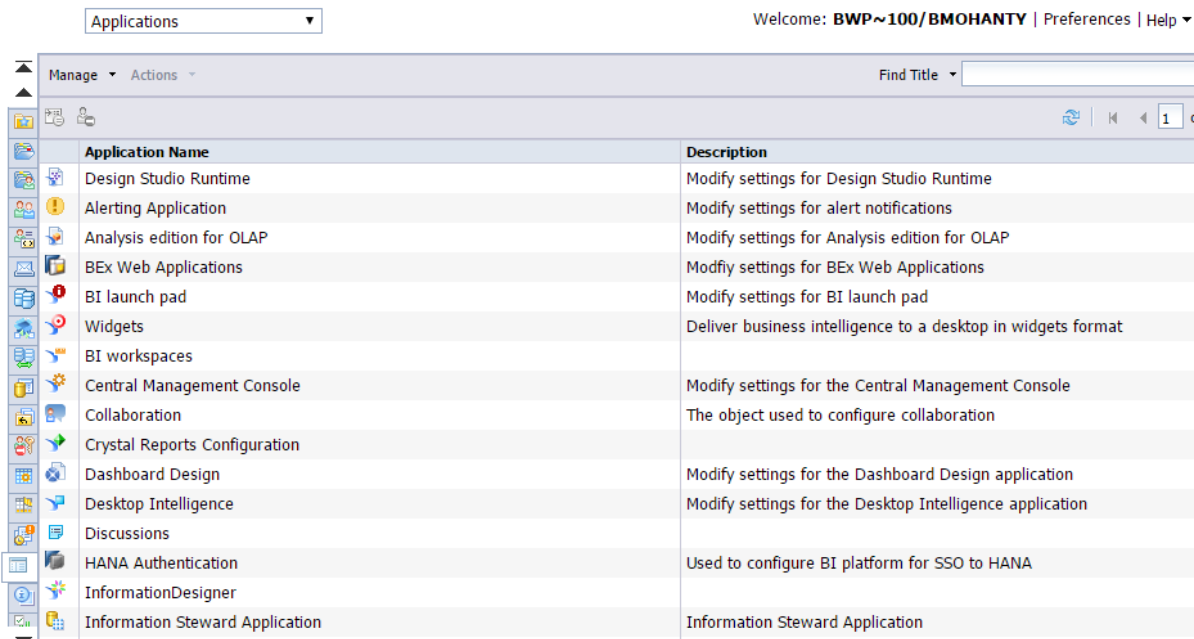


5 Application Level Security:

Users need access to particular Business Objects applications to perform their jobs effectively. Business Objects Administrator is responsible for setting appropriate application security levels according to the needs of our organization.

Application security is used to control the functionality that users and groups have to the Business Objects Enterprise applications. The Manage area of the CMC allows us to control access for the following Business Objects Enterprise applications:

Central Management Console



The screenshot shows the Central Management Console (CMC) interface. At the top, there is a navigation bar with "Applications" selected in a dropdown menu. The user is logged in as "BWP~100/BMOHANTY". Below the navigation bar, there is a "Manage" dropdown and an "Actions" dropdown. A search bar labeled "Find Title" is also present. The main content area displays a table with two columns: "Application Name" and "Description".

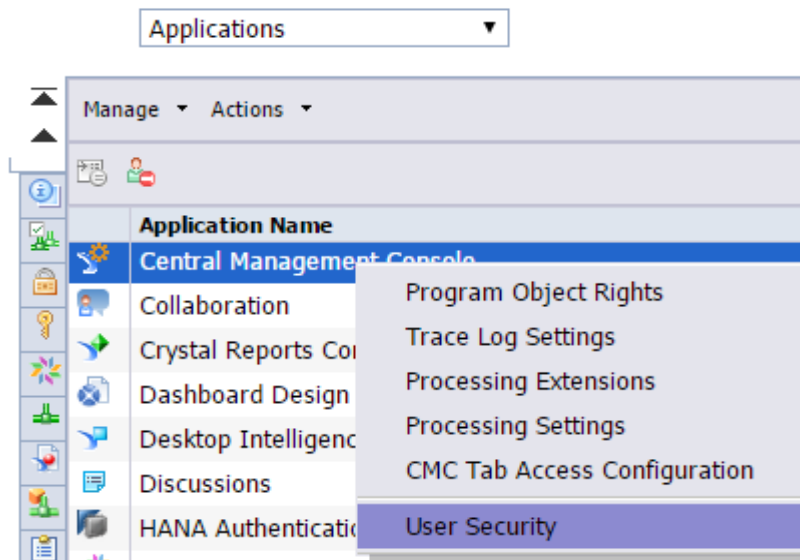
Application Name	Description
Design Studio Runtime	Modify settings for Design Studio Runtime
Alerting Application	Modify settings for alert notifications
Analysis edition for OLAP	Modify settings for Analysis edition for OLAP
BEx Web Applications	Modify settings for BEx Web Applications
BI launch pad	Modify settings for BI launch pad
Widgets	Deliver business intelligence to a desktop in widgets format
BI workspaces	
Central Management Console	Modify settings for the Central Management Console
Collaboration	The object used to configure collaboration
Crystal Reports Configuration	
Dashboard Design	Modify settings for the Dashboard Design application
Desktop Intelligence	Modify settings for the Desktop Intelligence application
Discussions	
HANA Authentication	Used to configure BI platform for SSO to HANA
InformationDesigner	
Information Steward Application	Information Steward Application

6 Manage CMC User Security

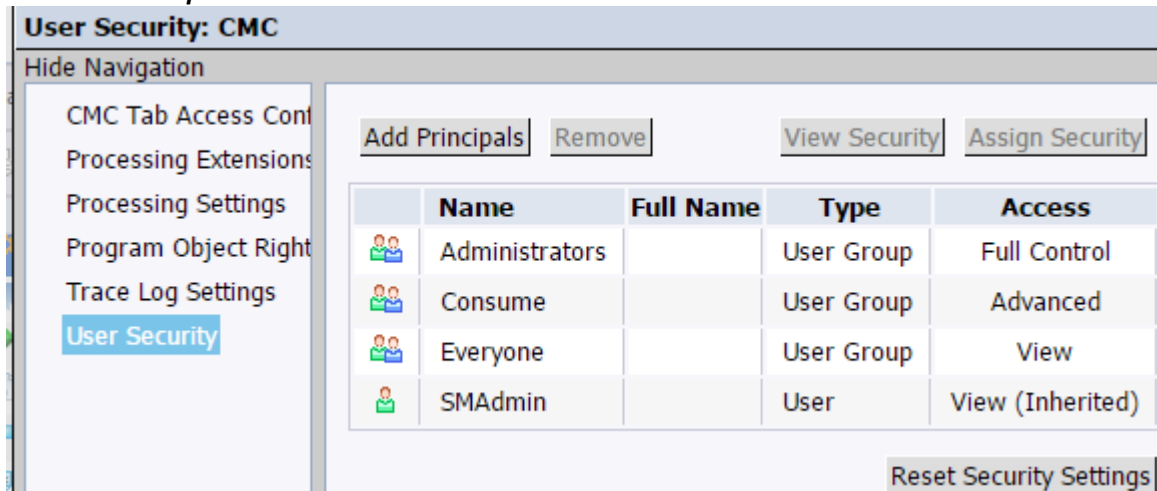
To Manage CMC security:

Logon to **CMC** -> Click **Applications** → Select **CMC** → Now Right Click → select **User Security**.

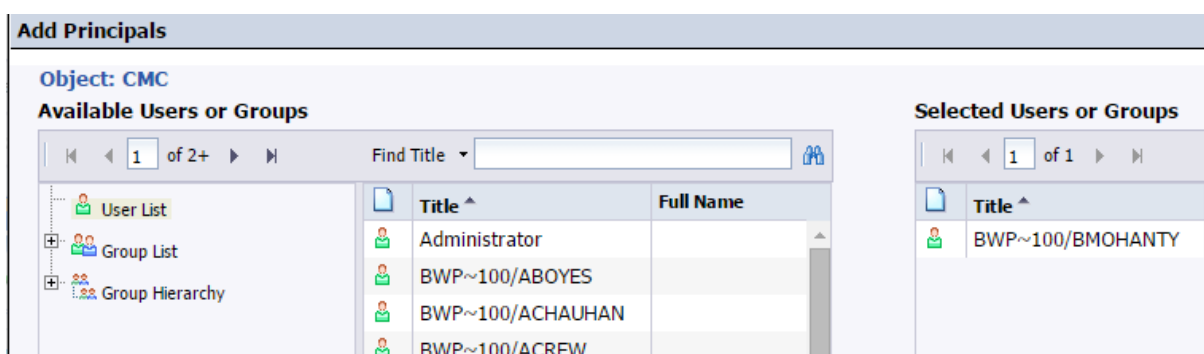
Central Management Console



Click **Add Principals**:

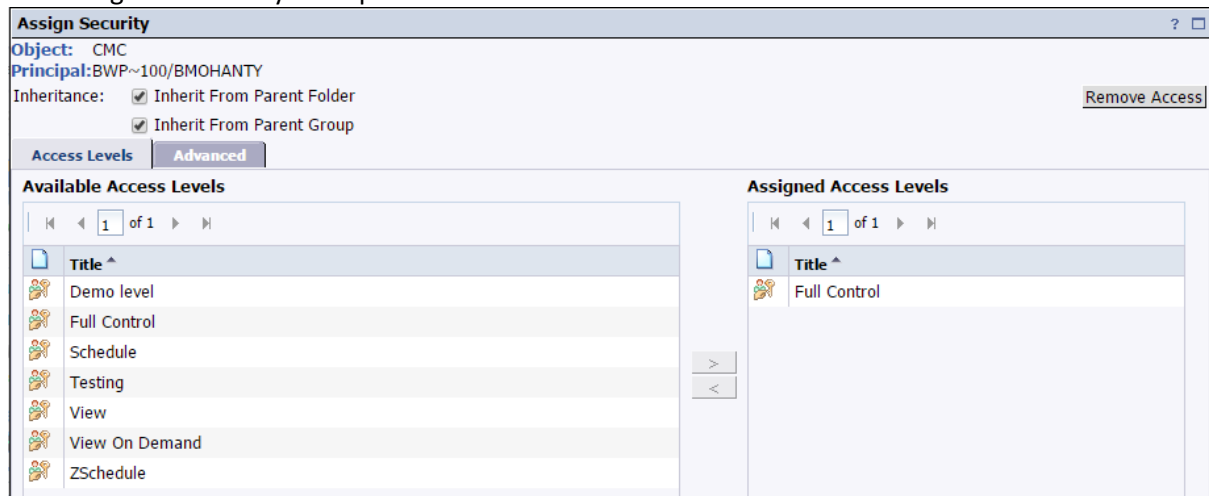


Select the principal for which we want to assign security.



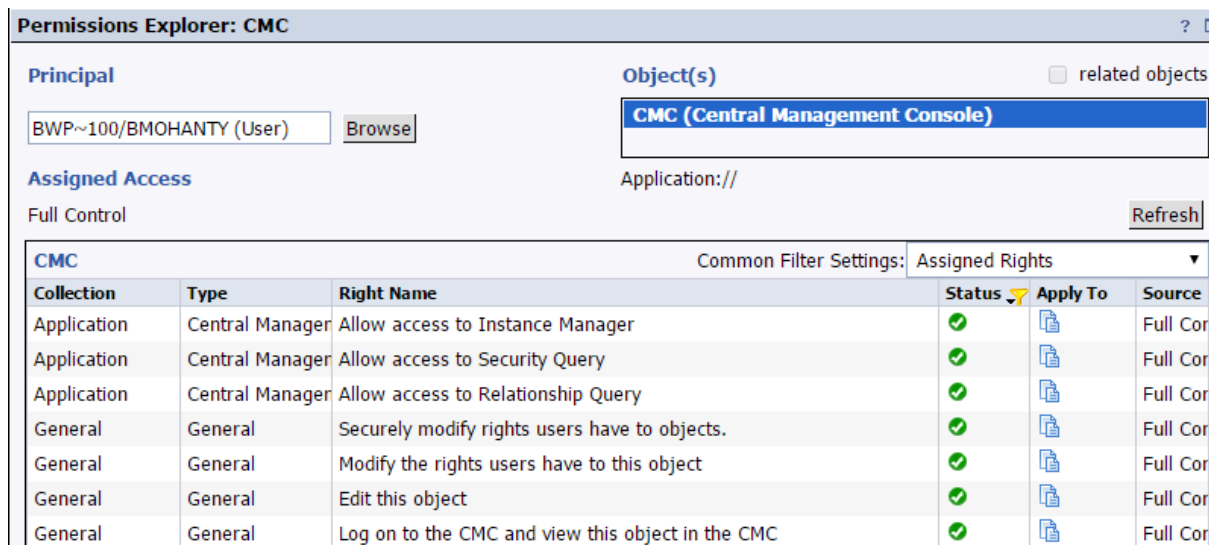
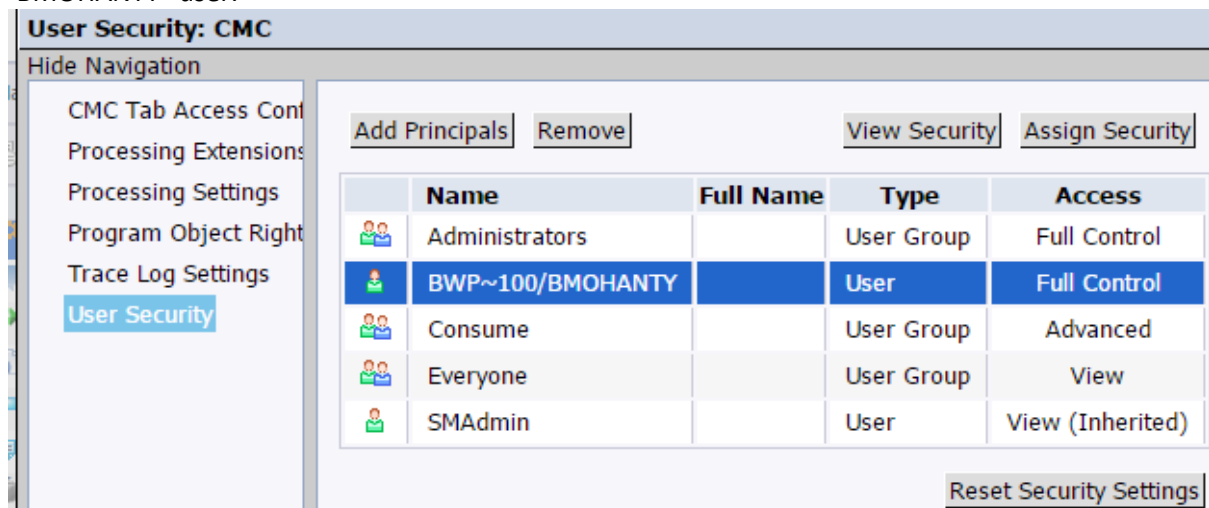
On the bottom right corner click "Add and Assign Security": **Add and Assign Security**.

Now assign the security as required:



Now Click **“Apply”** & **“Ok”**

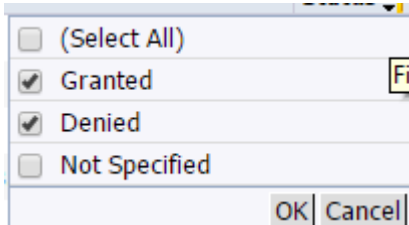
Now Click **“View Security”** on the Next screen to check what access has been provided to **“BMOHANTY”** user:



Similarly we can manage Security, and access for rest of the applications.

7 Advance Rights

We may sometimes need to override certain granular rights in an access level. Advanced rights let us customize the rights for a principal on top of the access levels, the principal already has. There are 3 Type of rights exist as explained earlier:



Exception:

- In general, the rights that are set on child objects override the rights that are set on parent Object.
- In general, the rights that are set on subgroups or members of groups override the rights that are set on groups.
- If a user belongs to more than one group, and there is a conflict in rights assignments between the groups to which the user belongs to, the Denied (D) right wins over a Granted (G) right, and the Granted (G) right wins over a Not Specified

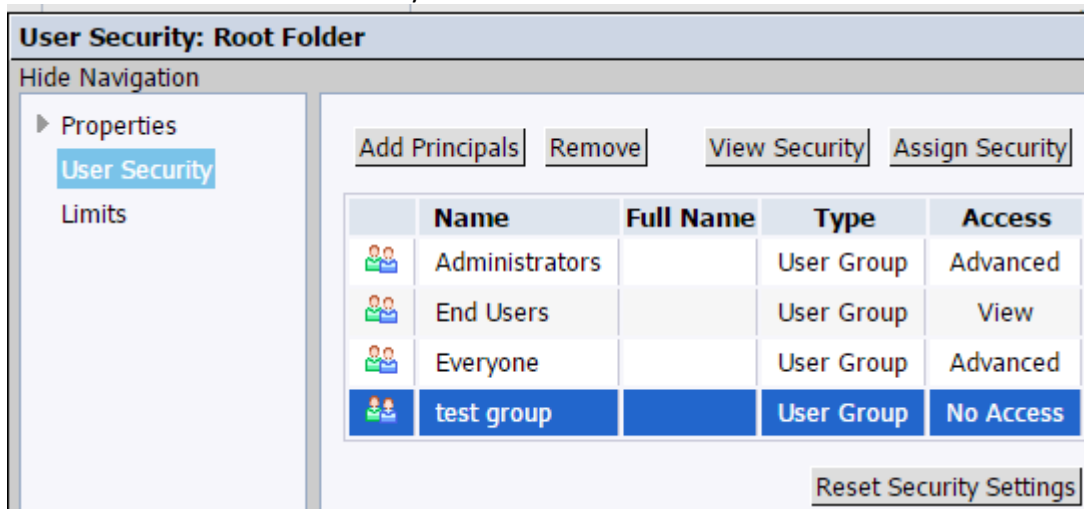
Examples: (Advanced Rights)

We will be discussing, how advanced rights are used through this example. Consider an example where our user needs to have following access:

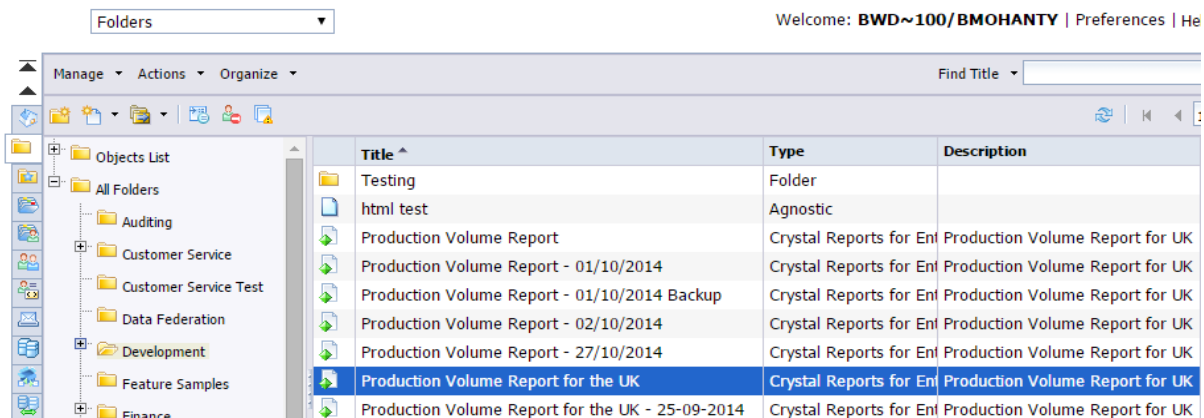
- Needs to be provided no access to any folder or report ,
- Need to have access to schedule a report (Material Plant) ,
- Need to view, pause and resume its scheduled instances
- Need to be restricted to delete a instance and view a report.

We proceed as below:

1. Maintain **No Access** at root level security at Folders:



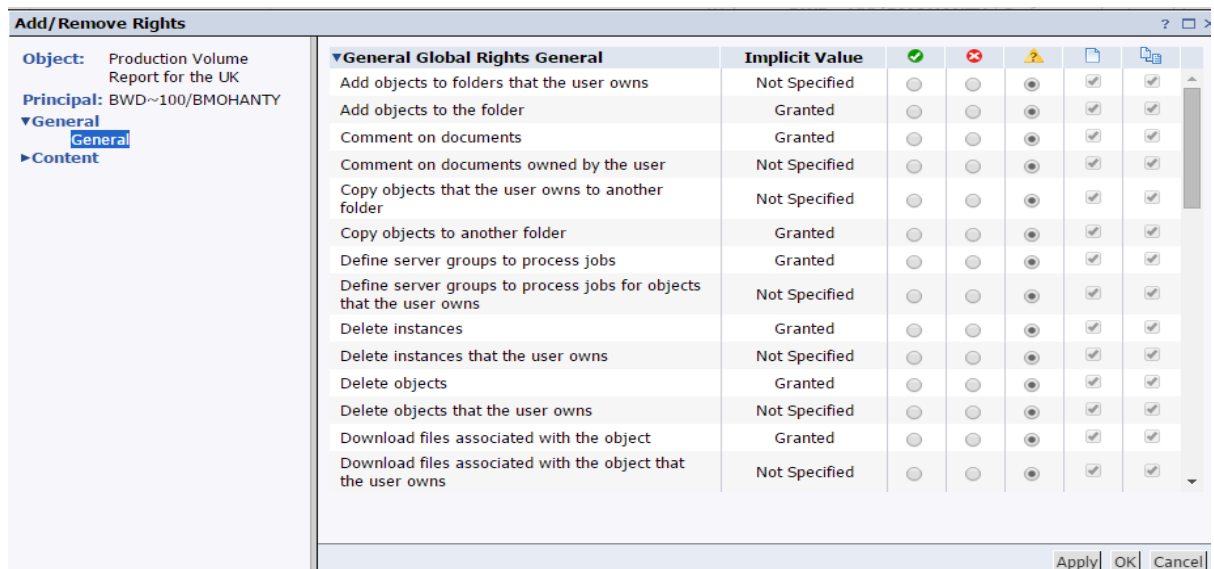
2. Select the "Production Volume Report for the UK" → Right clicks → **User Security**



Break inheritance and click **Advance** tab -> **Add/Remove Rights**



Once done, we are able to view the General global rights. Now maintain the rights by clicking on radio buttons for grant denied or not specified. Rights are divided into the following collections based on the object types they apply to:



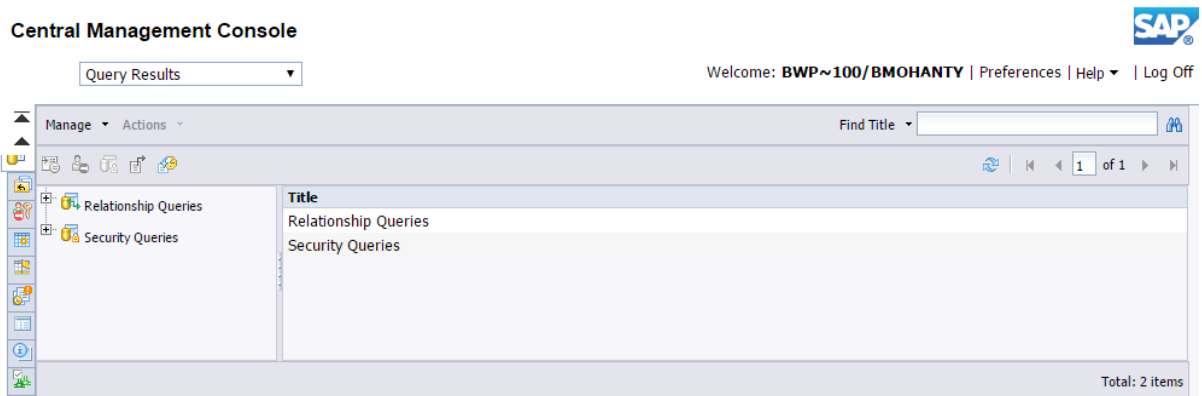
- Select the Grant radio button for providing access to schedule a report, view, pause and resume its Scheduled instances.
- Select Deny radio button to deny access to any folder or report, and to view, delete a report.
- We can also allow the rights to be applied to a Sub object, by checking the Object and Sub Object check boxes, next to the Rights column.
- Only after we click grant or deny radio button, object and sub-object check boxes are enabled. Now we can maintain the scope of rights.
- If we want to apply a right only for a folder and not for its sub folders, then uncheck sub-object check box.

8 Security Query

Due to the complexities inherent in a security system as complicated as Business Objects Enterprise, systems administrators sometimes find it difficult to pinpoint from where a particular user right is inherited.

Security queries let us determine which objects a principal has certain rights to and enables us to manage user rights:

In the earlier section of this document, we have created a group called "Power User - Finance". In this section we will find out what access "Power User - Finance" have on Servers using the "Security Query". For this: Logon to **CMC** -> Select "**Query Results**"



Now select **Security Queries** → Right click → Create **Security Query**.

Create Security Query

Query Principal

The query searches for objects for this principal:

Browse

Query Permission

The query searches for objects for which the above principal has all of these permissions:

Do not query by permissions Browse

Collection	Type	Right Name	
			X

Query Context

The query searches for objects only in these section(s) of the CMC:

Folders Browse

Query subobject

Folders Browse

Query subobject

Folders Browse

Query subobject

Folders Browse

Query subobject

Lets provide the required inputs as below:

- i) Principal (User / User Group).
 - ii) Check /Uncheck Query Permission as per the requirement.
 - iii) Select the Query Context (Servers)
- After selecting the required parameters click **OK**.
 - Now, the next screen appears showing the result regarding what access the *principal* has on the **Query context**.
 - We can also click on the **Source** column to view, from where the Principal is obtaining its access:

In case we see, the source along with (Inherited) it implies that access comes either from the Parent group or from the parent folder.

9 Appendix (BW Authorization Set up in Detail)

SAP BW "TEST" USERS

	User	Note	User Type	Application Area
1	DEVELOPER	New Test User	All Access User	Cross-Application
2	REPORTUSER	New Test User	All Access User	Cross-Application
3	POWERUSER	New Test User	All Access User	Cross-Application
4	CSRUSER	New Test User	Report User	Customer Services
5	CSPUSER	New Test User	Power User	Customer Services
6	SDRUSER	New Test User	Report User	Sales & Distribution
7	SDPUSER	New Test User	Power User	Sales & Distribution
8	FIRUSER	New Test User	Report User	Finance & Controlling
9	FIPUSER	New Test User	Power User	Finance & Controlling
10	FSCMRUSER	New Test User	Report User	Dispute Management
11	FSCMPUSER	New Test User	Power User	Dispute Management
12	SCMRUSER	New Test User	Report User	Supply Chain Management
13	SCMPUSER	New Test User	Power User	Supply Chain Management
14	PMRUSER	New Test User	Report User	Plant Maintenance
15	PMPUSER	New Test User	Power User	Plant Maintenance
16	MMRUSER	New Test User	Report User	Materials Management
17	MMPUSER	New Test User	Power User	Materials Management
18	MMRUSER	New Test User	Report User	Procurement
19	MMPUSER	New Test User	Power User	Procurement
20	ARRUSER	New Test User	Report User	Accounts Receivable
21	ARPUSER	New Test User	Power User	Accounts Receivable

SAP BW "POWERUSER" ROLES

	Roles	Note	Purpose
11	ZBW_ACCOUNTS_RECEIVABLE_EXEC_T	New Test Role	Accounts Receivable Queries
12	ZBW_CUSTOMER_SERV_QUERY_EXEC_T	New Test Role	Customer Services Queries
13	ZBW_FICO_QUERY_EXEC_T	New Test Role	Finance & Controlling Queries
14	ZBW_MM_QUERY_EXEC_T	New Test Role	Materials Management Queries
15	ZBW_PROCUREMENT_QUERY_EXEC_T	New Test Role	Procurement Queries
16	ZBW_SD_QUERY_EXEC_T	New Test Role	Sales & Distribution Queries
17	ZBW_FSCM_QUERY_EXEC_T	New Test Role	Dispute Management Queries
18	ZBW_SUPPLY_CHAIN_EXEC_T	New Test Role	Supply Chain Queries
19	ZBW_PLANT_MAINTENENCE_EXEC_T	New Test Role	Plant Maintenance Queries

SAP BW "REPORTUSER" ROLES

	Roles	Note	Purpose
1	ZBWC_ACCTS_RECEIVABLE_EUSR_TST	New Test Role	Accounts Receivable Queries
2	ZBWC_CUSTOMER_SERVICE_EUSR_TST	New Test Role	Customer Services Queries
3	ZBWC_FICO_EUSR_TST	New Test Role	Finance & Controlling Queries
4	ZBWC_MM_EUSR_TST	New Test Role	Materials Management Queries
5	ZBWC_PROCUREMENT_EUSR_TST	New Test Role	Procurement Queries
6	ZBWC_SD_EUSR_TST	New Test Role	Sales & Distribution Queries

7	ZBWC_FSCM_EUSR_TST	New Test Role	Dispute Management Queries
8	ZBWC_SUPPLY_CHAIN_EUSR_TST	New Test Role	Supply Chain Queries
9	ZBWC_PLANT_MAINTENANC_EUSR_TST	New Test Role	Plant Maintenance Queries

SAP BW TEST” “ROLE” ASSIGNMENT TO different “USERS”

Access to ALL Report - Power Users (USER ID: POWERUSER)			
	Roles	Note	Purpose
1	CRYSTAL_ENTITLEMENT	Existing Role	
2	ZBW_ACCOUNTS_RECEIVABLE_EXEC_T	New Test Role	Accounts Receivable Queries
3	ZBW_CUSTOMER_SERV_QUERY_EXEC_T	New Test Role	Customer Services Queries
4	ZBW_FICO_QUERY_EXEC_T	New Test Role	Finance & Controlling Queries
5	ZBW_MM_QUERY_EXEC_T	New Test Role	Materials Management Queries
6	ZBW_PROCUREMENT_QUERY_EXEC_T	New Test Role	Procurement Queries
7	ZBW_SD_QUERY_EXEC_T	New Test Role	Sales & Distribution Queries
8	ZBW_FSCM_QUERY_EXEC_T	New Test Role	Dispute Management Queries
9	ZBW_SUPPLY_CHAIN_EXEC_T	New Test Role	Supply Chain Queries
10	ZBW_PLANT_MAINTENANCE_EXEC_T	New Test Role	Plant Maintenance Queries
11	ZBW_COMMON_USER_FUNCTIONS	Existing Role	
12	ZSAP_ECC_RFC_ROLE	Existing Role	

Commercial Finance Report Users (USER ID: CFRUSER)			
	Roles	Note	Purpose
1	CRYSTAL_ENTITLEMENT	Existing Role	
2	ZBWC_ACCTS_RECEIVABLE_EUSR_TST	New Test Role	Accounts Receivable Queries
3	ZBWC_CUSTOMER_SERVICE_EUSR_TST	New Test Role	Customer Services Queries
4	ZBWC_FICO_EUSR_TST	New Test Role	Finance & Controlling Queries
5	ZBW_COMMON_USER_FUNCTIONS	Existing Role	
6	ZSAP_ECC_RFC_ROLE	Existing Role	

Commercial Finance Power Users (USER ID: CFPUSER)			
	Roles	Note	Purpose
1	CRYSTAL_ENTITLEMENT	Existing Role	
2	ZBW_ACCOUNTS_RECEIVABLE_EXEC_T	New Test Role	Accounts Receivable Queries
3	ZBW_CUSTOMER_SERV_QUERY_EXEC_T	New Test Role	Customer Services Queries
4	ZBW_FICO_QUERY_EXEC_T	New Test Role	Finance & Controlling Queries
5	ZBW_COMMON_USER_FUNCTIONS	Existing Role	
6	ZSAP_ECC_RFC_ROLE	Existing Role	

Procurement Report Users (USER ID: PRRUSER)			
	Roles	Note	Purpose
1	CRYSTAL_ENTITLEMENT	Existing Role	
2	ZBWC_PROCUREMENT_EUSR_TST	New Test Role	Procurement Queries
3	ZBW_COMMON_USER_FUNCTIONS	Existing Role	
4	ZSAP_ECC_RFC_ROLE	Existing Role	

Procurement Power Users (USER ID: PRPUSER)			
	Roles	Note	Purpose
1	CRYSTAL_ENTITLEMENT	Existing Role	
2	ZBW_PROCUREMENT_QUERY_EXEC_T	New Test Role	Procurement Queries
3	ZBW_COMMON_USER_FUNCTIONS	Existing Role	
4	ZSAP_ECC_RFC_ROLE	Existing Role	

MM Report Users (USER ID: MMRUSER)			
	Role	Note	Purpose
1	CRYSTAL_ENTITLEMENT	Existing Role	
2	ZBWC_MM_EUSR_TST	New Test Role	Materials Management Queries
3	ZBW_COMMON_USER_FUNCTIONS	Existing Role	
4	ZSAP_ECC_RFC_ROLE	Existing Role	

MM Power Users (USER ID: MMPUSER)			
	Roles	Note	Purpose
1	CRYSTAL_ENTITLEMENT	Existing Role	
2	ZBW_MM_QUERY_EXEC_T	New Test Role	Materials Management Queries
3	ZBW_COMMON_USER_FUNCTIONS	Existing Role	
4	ZSAP_ECC_RFC_ROLE	Existing Role	

Customer Services Report Users (USER ID: CSRUSER)			
	Roles	Note	Purpose
1	CRYSTAL_ENTITLEMENT	Existing Role	
2	ZBWC_CUSTOMER_SERVICE_EUSR_TST	New Test Role	Customer Services Queries
3	ZBW_COMMON_USER_FUNCTIONS	Existing Role	
4	ZSAP_ECC_RFC_ROLE	Existing Role	

Customer Services Power Users (USER ID: CSPUSER)			
	Roles	Note	Purpose
1	CRYSTAL_ENTITLEMENT	Existing Role	
2	ZBW_CUSTOMER_SERV_QUERY_EXEC_T	New Test Role	Customer Services Queries
3	ZBW_COMMON_USER_FUNCTIONS	Existing Role	
4	ZSAP_ECC_RFC_ROLE	Existing Role	

Finance Report Users (USER ID: FIRUSER)			
	Roles	Note	Purpose
1	CRYSTAL_ENTITLEMENT	Existing Role	
2	ZBWC_FICO_EUSR_TST	New Test Role	Finance & Controlling Queries
3	ZBW_COMMON_USER_FUNCTIONS	Existing Role	
4	ZSAP_ECC_RFC_ROLE	Existing Role	

Finance Services Power Users (USER ID: FIPUSER)			
	Roles	Note	Purpose
1	CRYSTAL_ENTITLEMENT	Existing Role	
2	ZBW_FICO_QUERY_EXEC_T	New Test Role	Finance & Controlling Queries
3	ZBW_COMMON_USER_FUNCTIONS	Existing Role	
4	ZSAP_ECC_RFC_ROLE	Existing Role	

Accounts Receivable Report Users (USER ID: ARRUSER)			
	Roles	Note	Purpose
1	CRYSTAL_ENTITLEMENT	Existing Role	
2	ZBWC_ACCTS_RECEIVABLE_EUSR_TST	New Test Role	Accounts Receivable Queries
3	ZBW_COMMON_USER_FUNCTIONS	Existing Role	
4	ZSAP_ECC_RFC_ROLE	Existing Role	

Accounts Payable Power Users (USER ID: ARPUSER)			
	Roles	Note	Purpose
1	CRYSTAL_ENTITLEMENT	Existing Role	
2	ZBW_ACCOUNTS_RECEIVABLE_EXEC_T	New Test Role	Accounts Receivable Queries
3	ZBW_COMMON_USER_FUNCTIONS	Existing Role	
4	ZSAP_ECC_RFC_ROLE	Existing Role	

Supply Chain Report Users (USER ID: SCMRUSER)			
	Roles	Note	Purpose
1	CRYSTAL_ENTITLEMENT	Existing Role	
2	ZBWC_SUPPLY_CHAIN_EUSR_TST	New Test Role	Supply Chain Queries
3	ZBW_COMMON_USER_FUNCTIONS	Existing Role	
4	ZSAP_ECC_RFC_ROLE	Existing Role	

Supply Chain Power Users (USER ID: SCMPUSER)			
	Roles	Note	Purpose
1	CRYSTAL_ENTITLEMENT	Existing Role	
2	ZBW_SUPPLY_CHAIN_EXEC_T	New Test Role	Supply Chain Queries
3	ZBW_COMMON_USER_FUNCTIONS	Existing Role	
4	ZSAP_ECC_RFC_ROLE	Existing Role	

Dispute Management Report Users (USER ID: FSCMRUSER)			
	Roles	Note	Purpose
1	CRYSTAL_ENTITLEMENT	Existing Role	
2	ZBWC_FSCM_EUSR_TST	New Test Role	Dispute Management Queries
3	ZBW_COMMON_USER_FUNCTIONS	Existing Role	
4	ZSAP_ECC_RFC_ROLE	Existing Role	

Dispute Management Power Users (USER ID: FSCMPUSER)			
	Roles	Note	Purpose
1	CRYSTAL_ENTITLEMENT	Existing Role	
2	ZBW_FSCM_QUERY_EXEC_T	New Test Role	Dispute Management Queries
3	ZBW_COMMON_USER_FUNCTIONS	Existing Role	
4	ZSAP_ECC_RFC_ROLE	Existing Role	

SD Report Users (USER ID: SDRUSER)			
	Role	Note	Purpose
1	CRYSTAL_ENTITLEMENT	Existing Role	
2	ZBWC_SD_EUSR_TST	New Test Role	Sales & Distribution Queries
3	ZBW_COMMON_USER_FUNCTIONS	Existing Role	
4	ZSAP_ECC_RFC_ROLE	Existing Role	

SD Power Users (USER ID: SDPUSER)			
	Roles	Note	Purpose
1	CRYSTAL_ENTITLEMENT	Existing Role	
2	ZBW_SD_QUERY_EXEC_T	New Test Role	Sales & Distribution Queries
3	ZBW_COMMON_USER_FUNCTIONS	Existing Role	
4	ZSAP_ECC_RFC_ROLE	Existing Role	

PM Report Users (USER ID: PMRUSER)			
	Role	Note	Purpose
1	CRYSTAL_ENTITLEMENT	Existing Role	
2	ZBWC_PLANT_MAINTENANC_EUSR_TST	New Test Role	Plant Maintenance Queries
3	ZBW_COMMON_USER_FUNCTIONS	Existing Role	
4	ZSAP_ECC_RFC_ROLE	Existing Role	

PM Power Users (USER ID: PMPUSER)			
	Roles	Note	Purpose
1	CRYSTAL_ENTITLEMENT	Existing Role	
2	ZBW_PLANT_MAINTENANCE_EXEC_T	New Test Role	Plant Maintenance Queries
3	ZBW_COMMON_USER_FUNCTIONS	Existing Role	
4	ZSAP_ECC_RFC_ROLE	Existing Role	

Developer (USER ID: DEVELOPER)			
	Roles	Note	Purpose
1	CRYSTAL_ENTITLEMENT	Existing Role	
2	SAP_J2EE_ADMIN	Existing Role	
3	ZBC_ECC_RSA1	Existing Role	
4	ZBW_COMMON_USER_FUNCTIONS	Existing Role	
5	ZBW_ACCOUNTS_RECEIVABLE_EXEC_T	New Test Role	Accounts Receivable Queries
6	ZBW_CUSTOMER_SERV_QUERY_EXEC_T	New Test Role	Customer Services Queries
7	ZBW_FICO_QUERY_EXEC_T	New Test Role	Finance & Controlling Queries
8	ZBW_MM_QUERY_EXEC_T	New Test Role	Materials Management Queries

9	ZBW_PROCUREMENT_QUERY_EXEC_T	New Test Role	Procurement Queries
10	ZBW_SD_QUERY_EXEC_T	New Test Role	Sales & Distribution Queries
11	ZBW_FSCM_QUERY_EXEC_T	New Test Role	Dispute Management Queries
12	ZBW_SUPPLY_CHAIN_EXEC_T	New Test Role	Supply Chain Queries
13	ZBW_PLANT_MAINTENENCE_EXEC_T	New Test Role	Plant Maintenance Queries
14	ZSAP_ECC_RFC_ROLE	Existing Role	