OBIEE Agency Administrator Guide

OBIEE Components Overview

There are two main metadata components within OBIEE:

- **OBIEE Repository** – this is where the tables are joined and placed into subject areas for users to access. The repository also ensures that data security (such as row-level and column-level security) is applied. The repository also identifies which users are allowed to run reports against an OBIEE subject area.
- **OBIEE Web Catalog** – this is where the folders, reports (called analyses), and dashboards reside. There are two types of security within the catalog:
  - **Tool privileges** – what functionality is available to you when using OBIEE, such as the ability to create dashboards, use specific views in your analyses, create Agents (a.k.a. iBots), etc.
  - **Catalog object permissions** – which folders, dashboards, and analyses you have access to view, edit, and delete, as well as which subject areas you have access to see when creating a new analysis.

  At the State of MN you gain access to both types of privileges based upon your SWIFT warehouse (EPM) role assignments. The warehouse roles used for catalog security were created in PeopleSoft just for this purpose.

Agency Administrator Functions

OET (previously MMB) has staff that is responsible for managing the OBIEE Repository and the OBIEE Web Catalog security. However, the ability to manage the subfolders, dashboards and reports within a shared agency folder has been given to agency administrators. Anyone with the agency-specific Agency Administrator warehouse role can manage the permissions within that agency folder.

You can request this role using the standard SWIFT security forms.

Examples of Catalog Permissions Roles

(XXX is replaced with an agency # and there is one of each of these roles for each agency using OBIEE).

The permissions described below are the defaults, but the agency administrator has the rights to change default permissions within their agency as they see fit.

- M_EPM_XXX_BASIC_RPT_DEVELOPER – Has access to navigate within the shared agency folder and access the reports and dashboards within it.
- M_EPM_XXX_ADV_RPT_DEVELOPER – Has access to navigate within the shared agency folder and access the reports and dashboards within it. Also has the ability to save reports into the Development subfolder for its agency.
- M_EPM_XXX_DASHBOARD_DEVELOPER – Has access to navigate within the shared agency folder and access the reports and dashboards within it. Also has the ability to save reports and dashboards into the agency folder and subfolders.
- M_EPM_XXX_AGY_ADMINISTRATOR – Has full control of the agency folder, subfolders and all contents. Can set permissions and create additional subfolders. The agency user is also responsible for requesting additional catalog roles for its agency, should they be needed for more flexible security within the agency folder than the default security provides.

## Instructions to Change Permissions within OBIEE

1. Login to OBIEE (via the Warehouse Reporting link within the SWIFT Portal).
2. Click the Catalog on the toolbar at the top.

3. Review the screenshot below. Each user will have "My Folders" which are their personal folders. No one else can see the contents of another user's personal folder. The "Shared Folders" are separated into a _Statewide folder at the top, which contains reports accessible to all agencies and individual agency folders, which can only be seen by those users having a warehouse role specific to that agency (e.g. anyone with the M_EPM_T79_ADV_RPT_DEVELOPER or one of the other T79 catalog roles will have access to the Transportation Department agency subfolder).
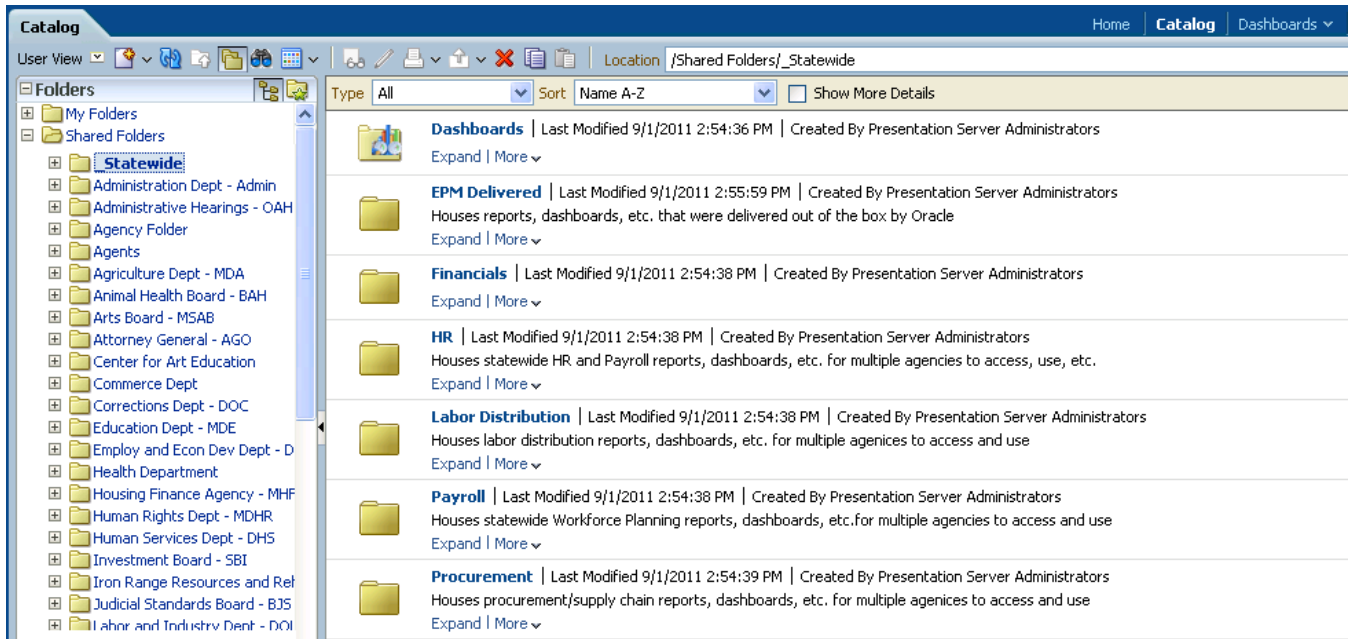

4. Note that within an agency folder a default subfolder has been created called "Development". By default the Advanced Report Developer and Dashboard Developer roles have access to save into this folder, but the Basic Report Developer cannot save to it or see its contents.
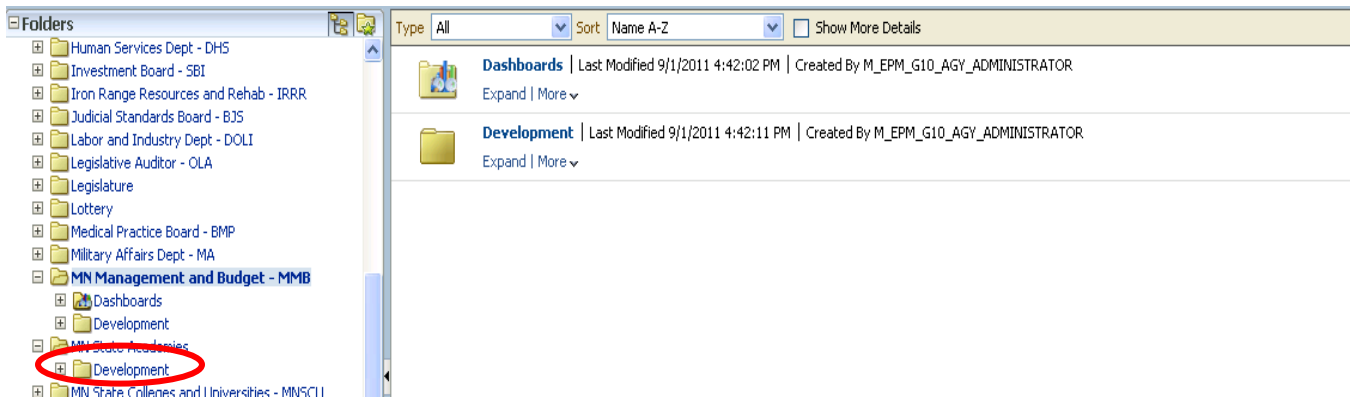
5. Note that another subfolder called "Dashboards" will appear, but only once a dashboard has been saved into the root agency folder. BY default those with a Dashboard Developer role can save in the root directory but Basic and Advanced Report Developers can only see the contents of the root folder. Those roles do not have access to save in the root folder.
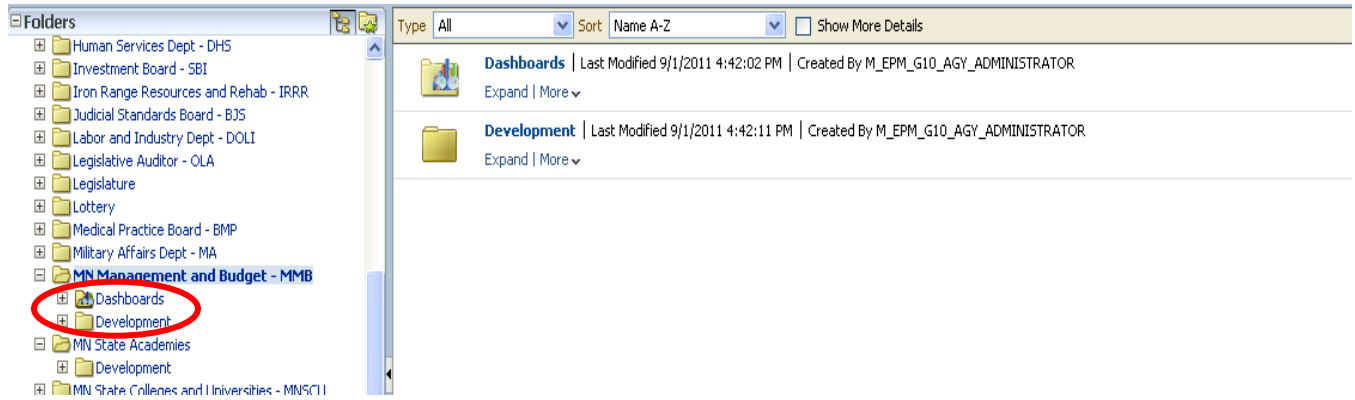

6. Be aware that only those dashboards saved in the Dashboards subfolder will appear on the Dashboards dropdown list. Dashboards located in other directories will not appear on the dropdown, but are accessible from the catalog.
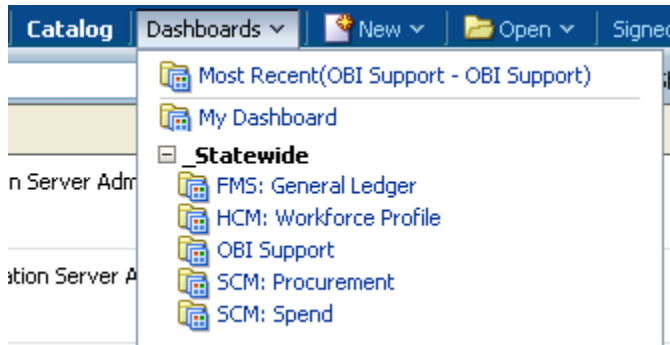

7. The recommendation is to use the Development folder to store work in progress analyses and dashboards, and then move them out to the root of the agency folder when they are ready for other users to access. However, you can create any subfolder structure you need. To create a new folder, click the folder you'd like the subfolder to reside in and then click the "New" button at the top of the folder list. Select the "Folder" option.
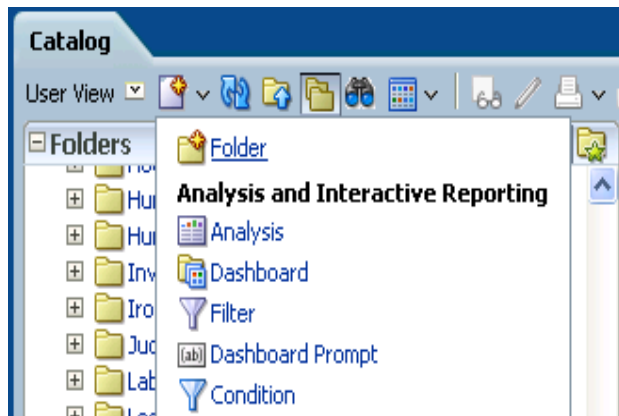
8. Once you create new folders you can set permissions for the folder by clicking the "More" dropdown menu located underneath the folder and choosing "Permissions" or by clicking the folder in the catalog and selecting "Permissions" from the Tasks options listed beneath the catalog list.
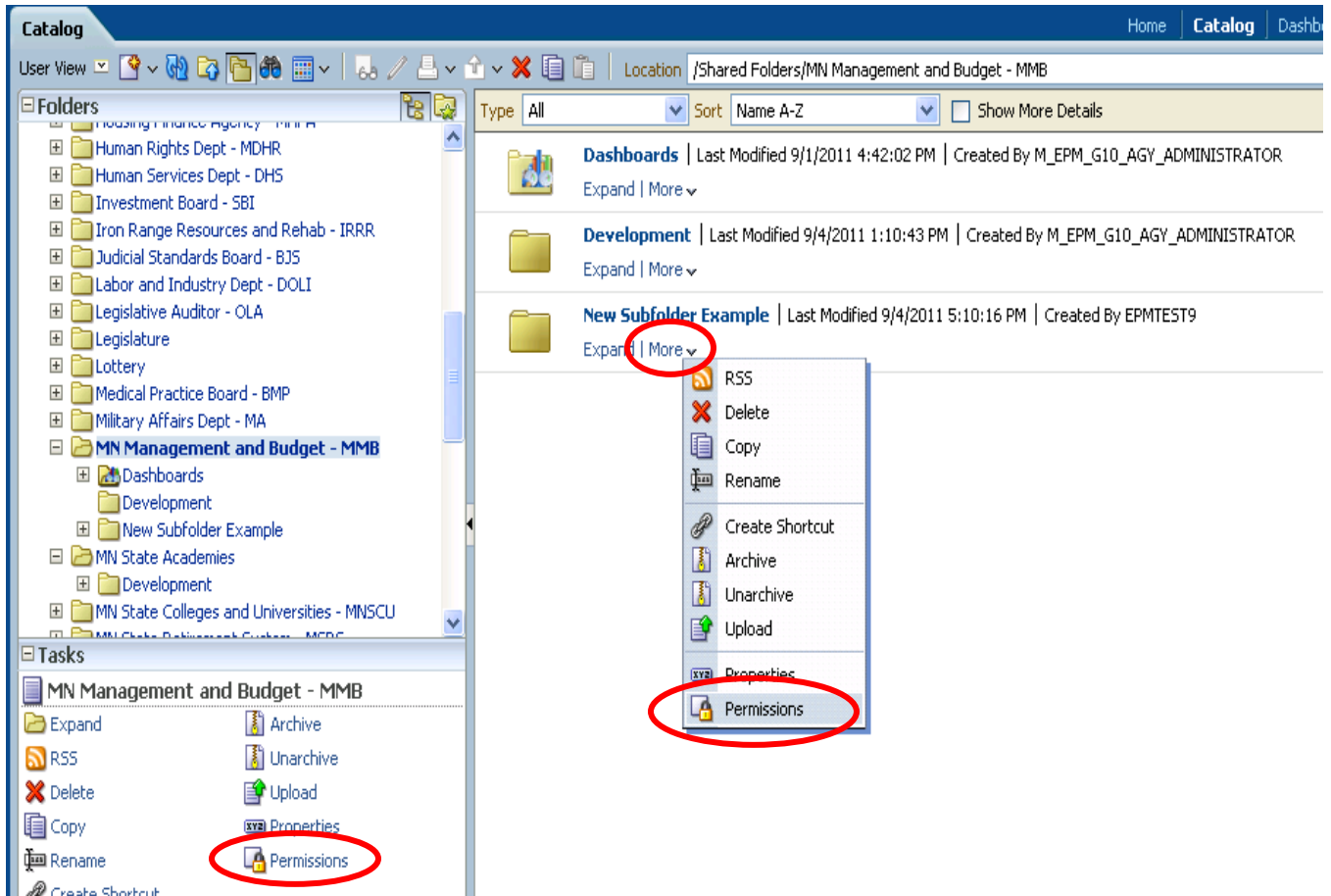

9. Note the folder may automatically pickup the permissions of its parent folder.
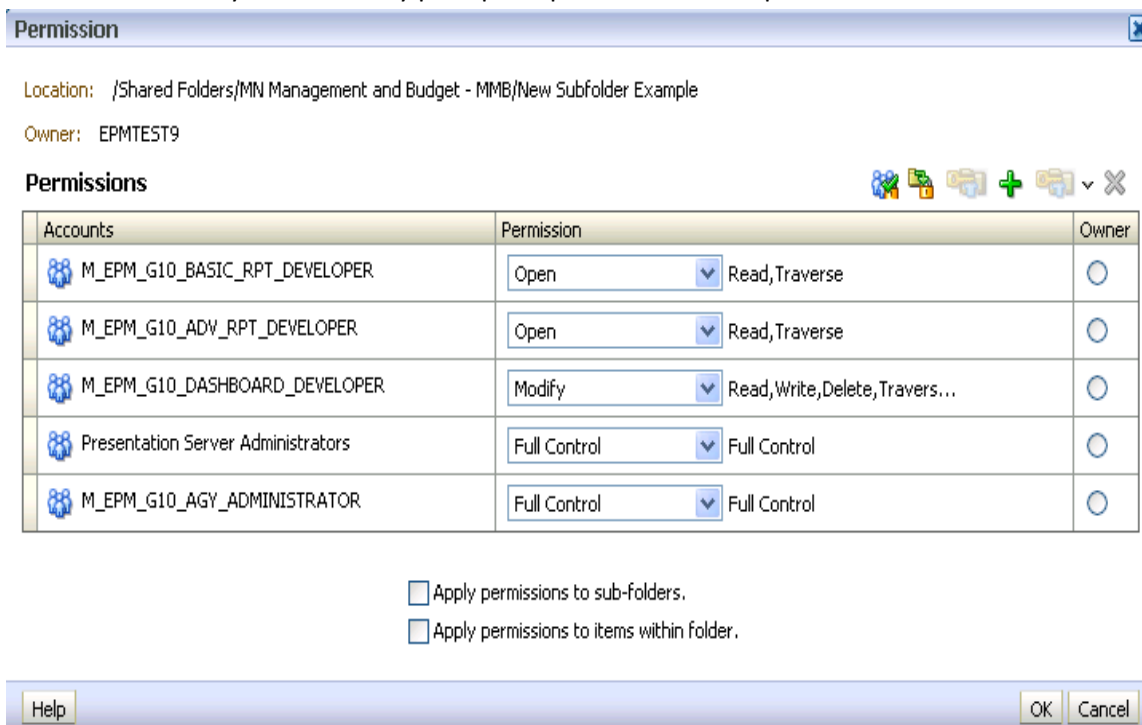
10. **To delete permissions** from a specific catalog group, select the catalog and click the "X" button in the upper right corner.
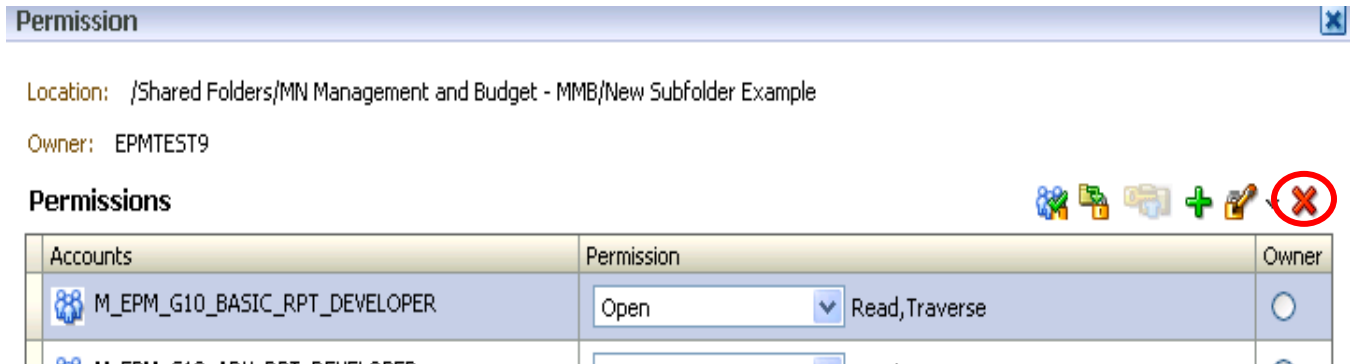

11. **To change permissions** from a specific catalog group, choose the permission dropdown menu and change accordingly. You may also want to apply the permissions to any subfolders of the folder you are setting permissions for and/or any items within the folder, such as dashboards or analyses. You can do that by checking the appropriate checkboxes at the bottom of the permission dialog.
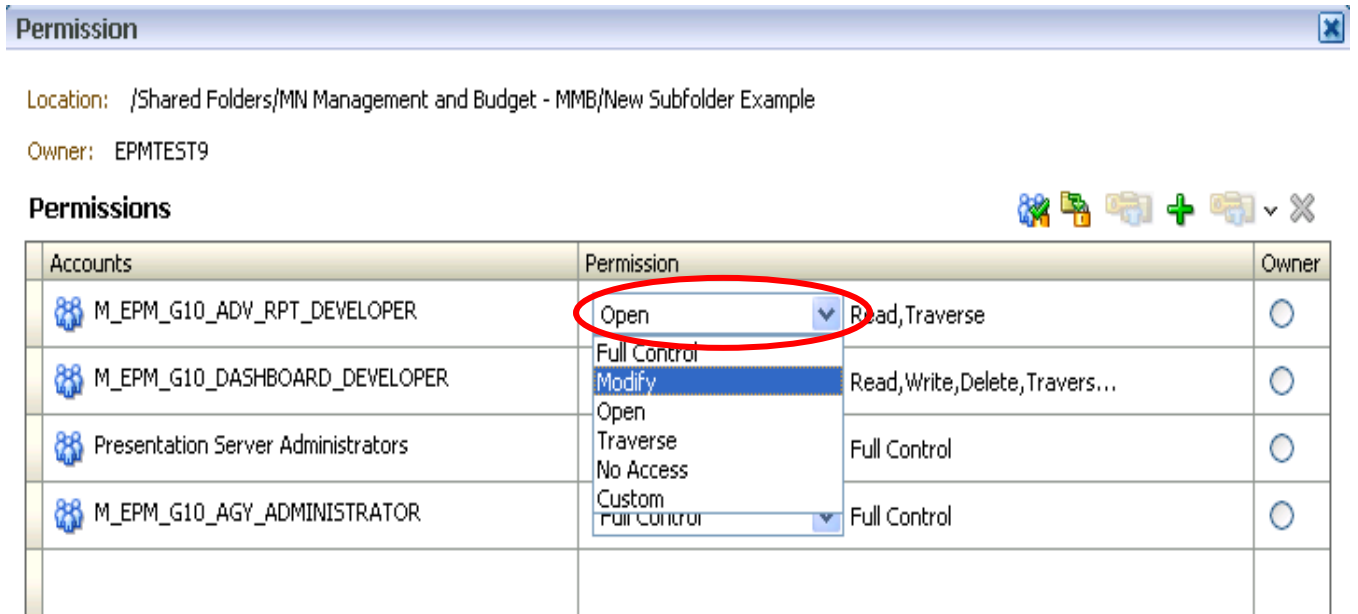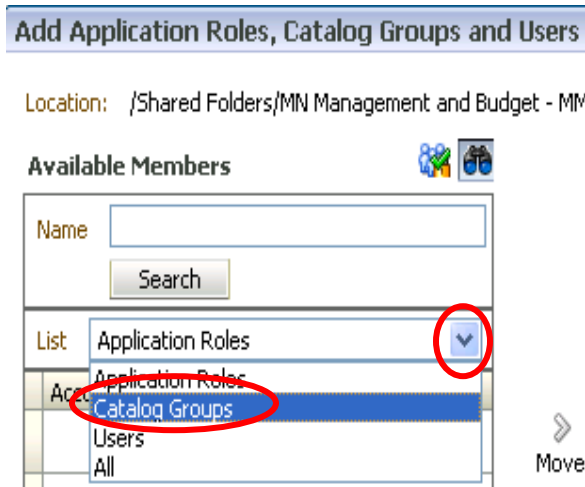
12. **To add permissions** to a new catalog group, click the "+" sign in the upper right corner.
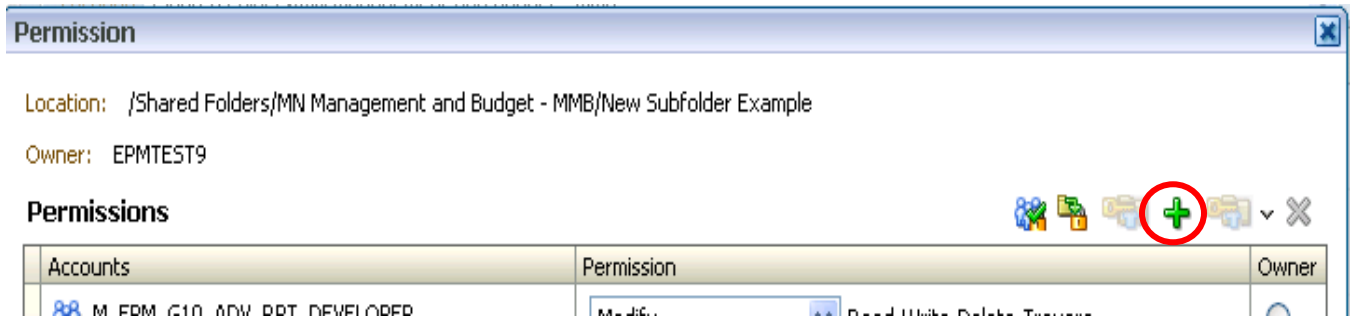
13. Click the "Catalog Groups" option from the List box so that you can search through a catalog group.

14. Enter a portion of the name in the "Name" field, using an "*" as a wildcard character. Then click "Search".

15. Select the specific groups you want to give permissions to and click the "Move" button. You can also set the permissions in this dialog or back at the Permission dialog.
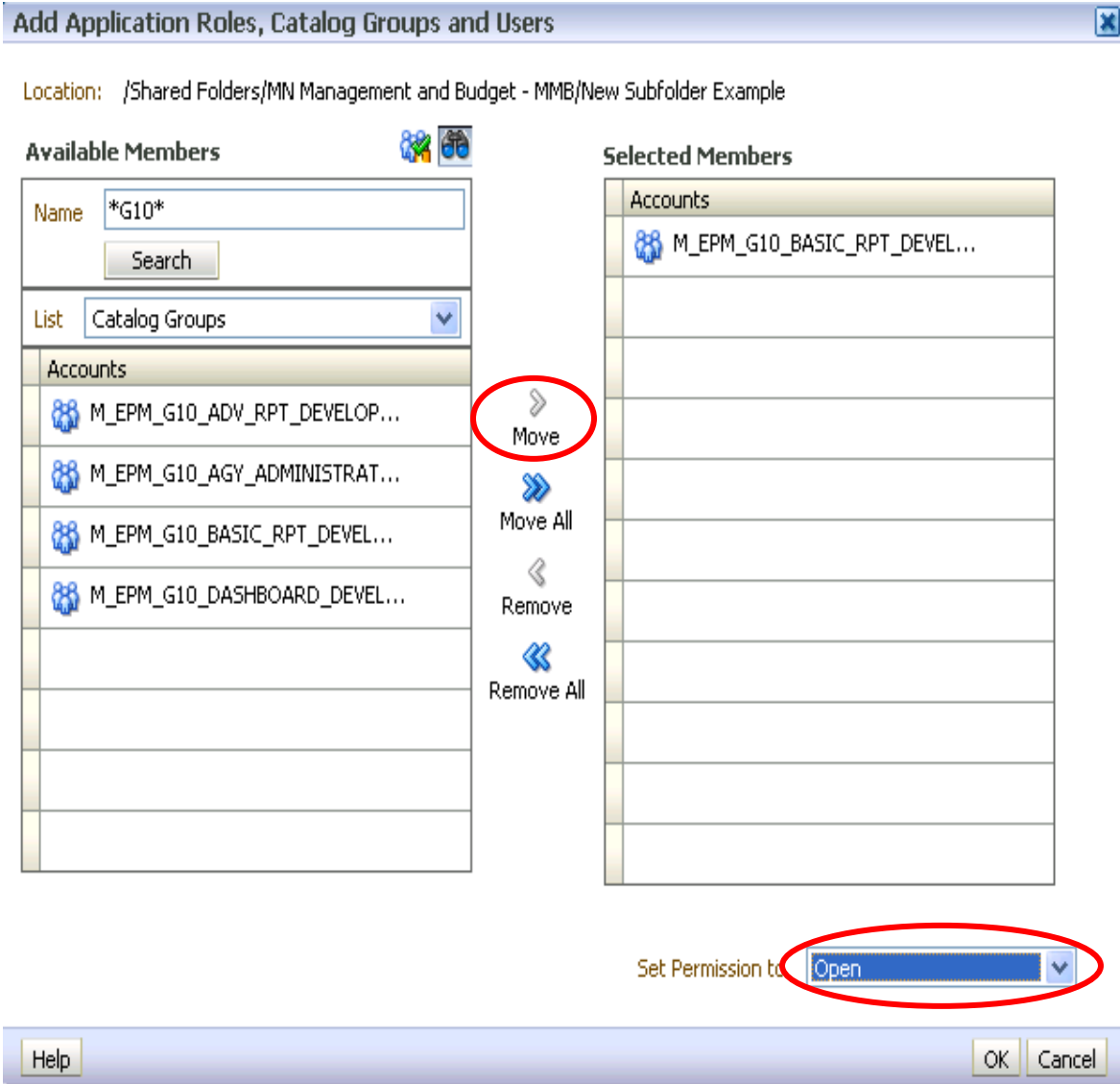

16. When you've selected all the catalog groups you want to establish permissions for, click "OK".
17. You'll see the additional catalog group listed. If you want to apply all the permissions you see to the subfolders and/or subfolder items then click the appropriate checkboxes. When you are done with the permissions click "OK".

18. You can also set security permissions on individual items such as analyses, dashboards, filters, and dashboard prompts. To do so, simply click the "More" dropdown menu on the specific item and select the "Permissions" option. Then establish permissions as described above.
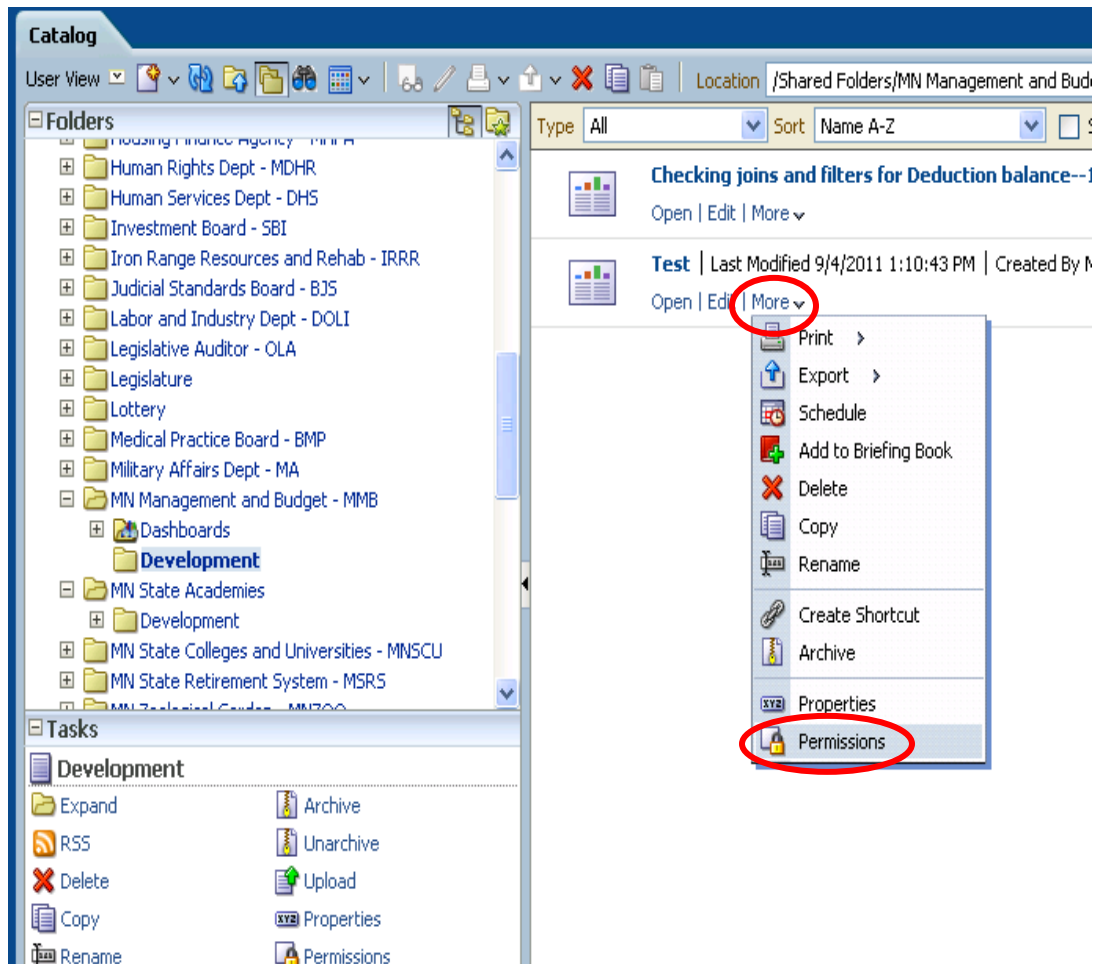
19. Be aware that you can configure your catalog view in a number of different ways using the buttons on the toolbar above the folder list. One of the most common ways is to click the "Change list view type" button. There is also a User View and Admin View that shows a slightly different catalog layout.
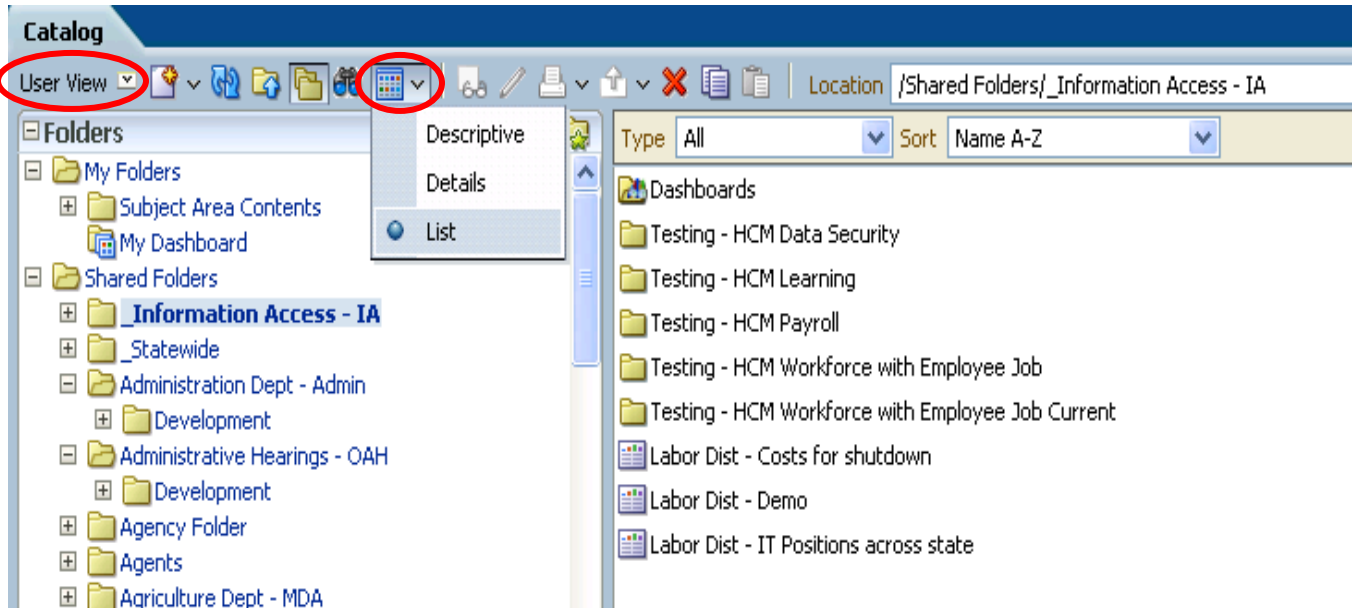
Understanding Permission Options
(from Oracle documentation)

These can be applied to folders or items within a folder:
No Access - Denies the user or group access to the item. Explicitly denying access takes precedence over any other permission.
Read - Allows the user or groups to view the item, but not make any changes.
Traverse - Allows the user or groups to access objects in folders within the selected folder when the user does not have permission to the selected folder. Example: The user is granted Traverse permission to the /shared/test folder. The user cannot access objects in the /shared/test folder, but can access objects stored in lower-level folders, such as /shared/test/guest.
Change/Delete - Allows the user or group to view, change, or delete the item.
Full Control - Allows the user or group to have full control over the item. This is the level of authority granted by default to the Administrator.

Do You Need New Catalog Groups?
It is likely that as your OBIEE user base increases within your agency you may need additional catalog groups to satisfy your folder security requirements. You can request additional catalog groups, but must stay with the naming standard of M_EPM_XXX_NameOfGroup with "XXX" being your agency number and "NameOfGroup" whatever identifying name you want the group to have so that you know what it is for (e.g. M_EPM_T79_MANAGERS).

To request a new catalog role, submit a ticket with the Help Desk providing the name of the new role and a list of user IDs you want to get the new role. You can access security forms using this link.
http://www.mmb.state.mn.us/access-forms