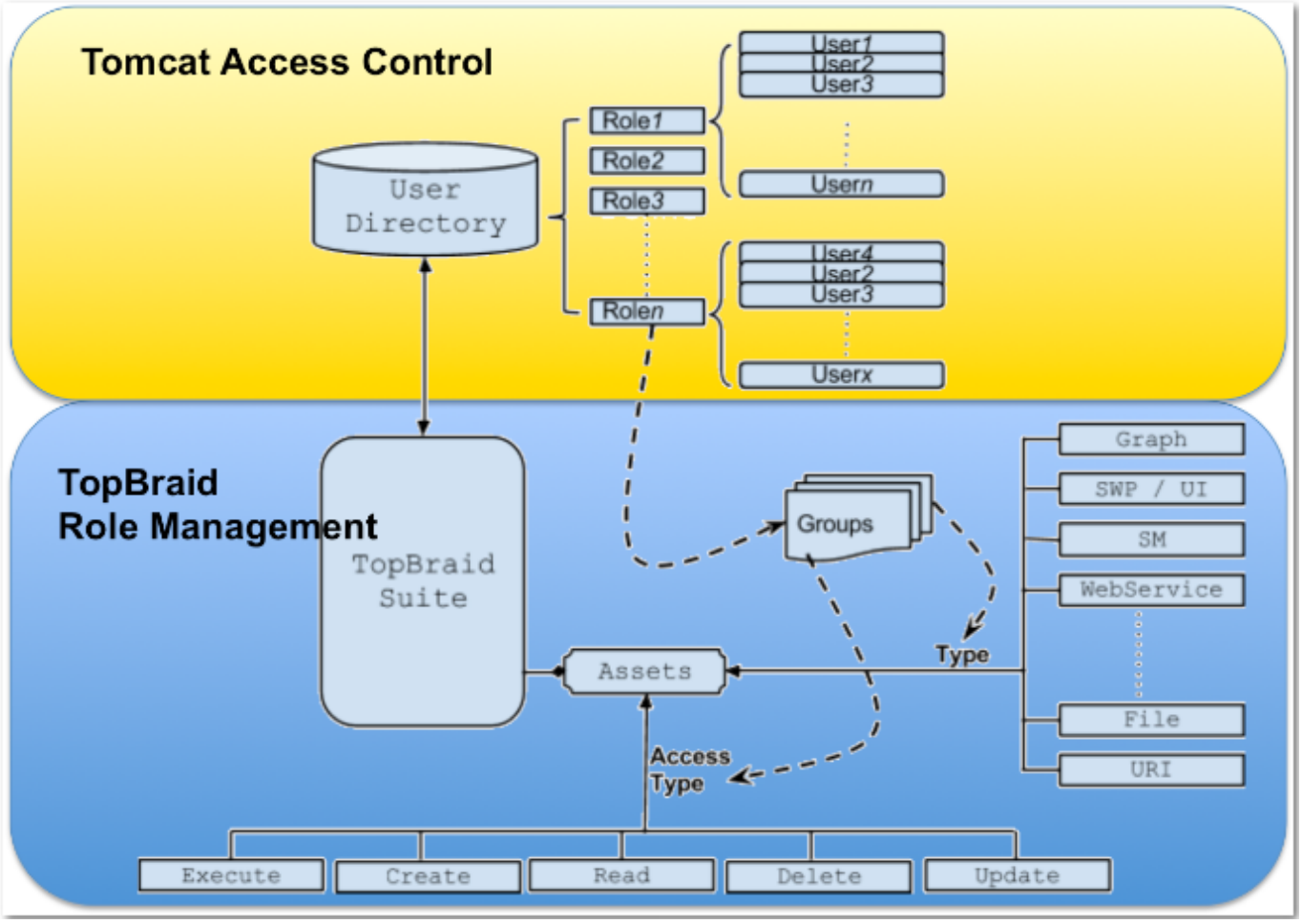
EVN Permission Group Management

Page Contents

The TopBraid Permission Group Management utility is found on the Server Administration page for all TopBraid server products. It provides a way to manage access controls to resources (e.g., graphs, files, projects, web services, etc.) from *non-teamwork-managed* origins (e.g., via external project uploads or send-transfers). Permission Groups are defined in Permission Group Management to associate the Groups to Roles defined in Tomcat Realms, such LDAP, LDAP/MS Active Directory, and Tomcat's in-memory user database (conf/tomcat-users.xml). The overall access control design is depicted in the diagram below. Note that Roles and user associations with Roles are defined outside of TopBraid product.

TopBraid Permission Group Management

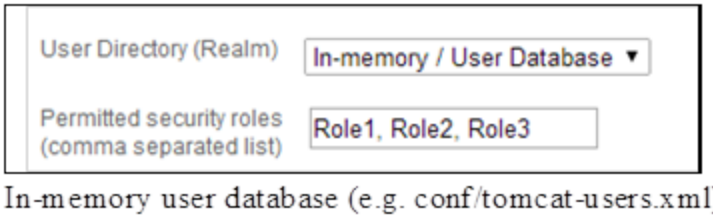


Installation and Admin Setup

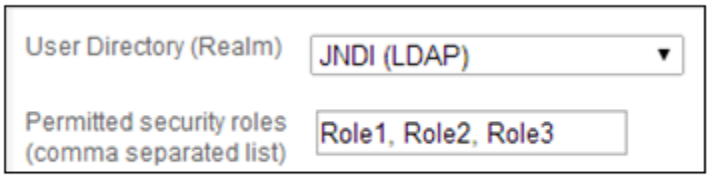
Initial role setup occurs during installation. Please refer to the Installation guide for the TopBraid Suite product you are using (EDG, EVN, TBI, TopBraid Live, etc.). For a Role to be used in a TopBraid server, the role must:

1. Be defined in a Tomcat/Realm, such as tomcat-users.xml/LDAP, and
2. Appear in the permitted security roles setup of the TopBraid (which define entries for security-constraint tags in the application's web. xml).

To define roles in the permitted security roles, enter a comma-delimited list of roles in the TopBraid Deployment Descriptor Configuration Page during installation. The following figures show the most common setups for LDAP and in-memory database (conf/tomcat-users.xml), where the role names in either case are Role1, Role2 and Role3. Note that these roles are defined in LDAP/Tomcat and are not editable from within TopBraid.



In-memory user database (e.g. conf/tomcat-users.xml)



LDAP User Directory

Access to the *Server Administration* page

Once installation is completed, the Server Administration page can be accessed by users associated with a role having access to the resource ANY_ROLE. The Permission Group Management page is found at Server Administration > Permission Group Management. This setup replaces the Superuser setting in versions of TopBraid Suite prior to version 4.4.

AdministratorGroup

TopBraid includes a default administrator group, named AdministratorGroup, which allows access to all resources. The group must be defined for at least one Role to prevent being locked out of the system. To remove AdministratorGroup for a specific role the user must define another role for the group. If AdministratorGroup is defined for at least one other role it can be removed from ANY_ROLE.

The Permission Group Management UI page: To navigate between them, click on the column name as shown in the following figure. Definitions for concepts appearing in this user interface are as follows:

- **Roles:** Roles are defined in LDAP/Tomcat and cannot be edited in this interface – a systems administrator will need to modify these using LDAP, tomcat-users.xml, etc. A role can be associated with one or more groups. If you update the tomcat-users.xml file to add more roles in the system, you must match such changes in the web.xml in the webapp folder.
- **Groups:** A group is defined within TBS and it identifies a group of resources, their respective access types and role/s defined in a user directory that it maps to.
- **Resource:** A resource is an instance of a resource that can be uniquely identified within TBS. Example of a resource is graph, SM script, an exposed Web service, a file etc. The approach controls access to individual resource or a group of resources.
- **Resource Permissions:** Each resource type allows a set of resource permissions. These permission types are **C**reate, **R**ead, **U**pdate, **D** elete and **E**xecute. E.g. for a graph CRUD access can be specified, for a SM script CRUD+E are relevant whereas for an exposed Web service only E access is relevant.

Defining new groups

To define a new permission group based on an existing role, first select a role, then click on the Add Group button and choose option New Group. Provide a name as shown in the figure and click 'Create Group' in the dialog. Groups can be associated with one or more resource with access permissions

Defining resource permissions

Resource permissions are defined with the **Add Resources** button in the figure below. Resource types are defined in Section 3. You can choose a listed wildcard resource or choose from a list of specific resources. In this example, we add a readAnyGraph group to a role (UpdateDenyRole). Then follow the menu from left to right to add Resources, Wildcards, or Projects as desired. Upon choosing the resource type the Permission Group Management view will display a set of permissions corresponding to the aforementioned CRUD+E resource permissions.

IMPORTANT:

When you want to 'remove' a group from a particular role – use the X icon next to the group name.

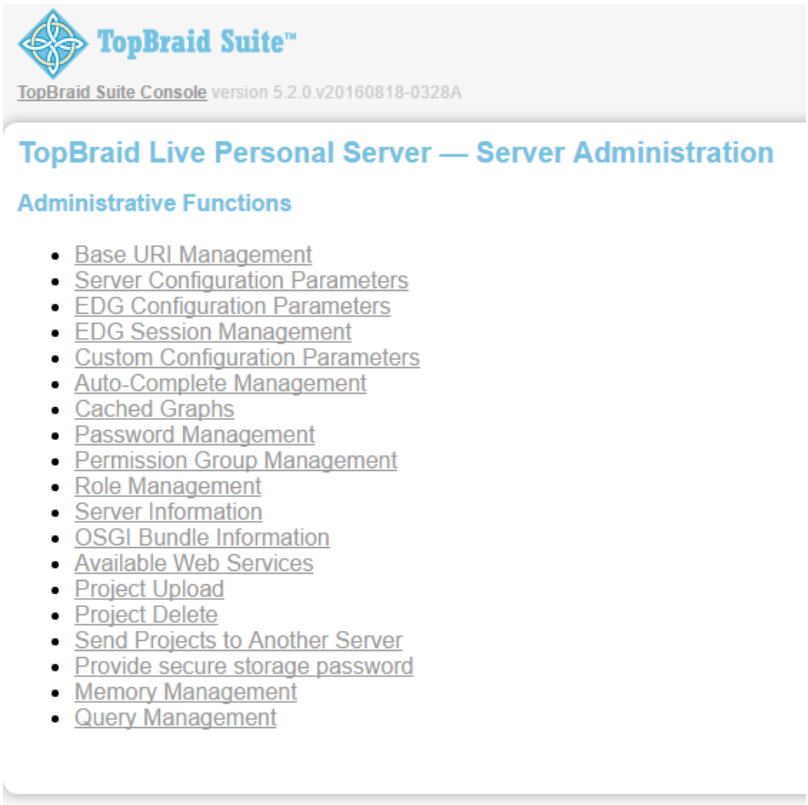
When you want to 'delete' a group completely – use the trashcan icon. (note that this will remove the group from all roles that were associated with it.

Project names should not contain a space - if they do you will get an error trying to expand them. Please correct Project name and reupload with no spaces.

Configure Permissions

Generally, roles are defined in a User Directory such as those defined in LDAP or Tomcat's in-memory user database. Each user should belong to a role in the system.

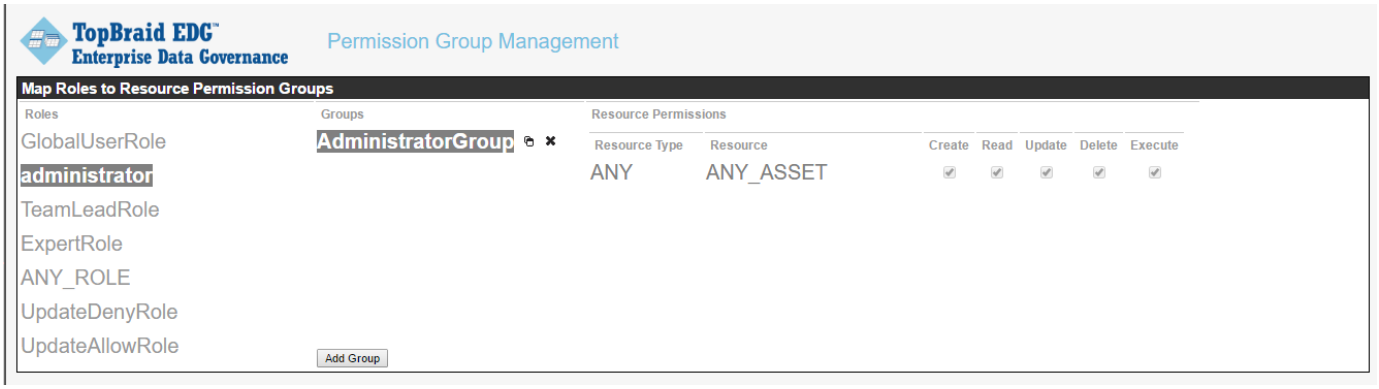
Choose Permission Group Management from the Administrative Functions Menu.



Choose a role from the "Roles" column:

AdministratorGroup is a system group that allows for administration access. Users belonging to role(s) that is assigned to this group will have administrative access. By Default, ANY_ROLE belongs to the AdministratorGroup. It's best to assign another role (e.g. 'administrator') to belong to 'AdministratorGroup' as shown above, so that you can remove the association of AdministratorGroup from ANY_ROLE when you install the system. This will prevent every user to have administrative functions.

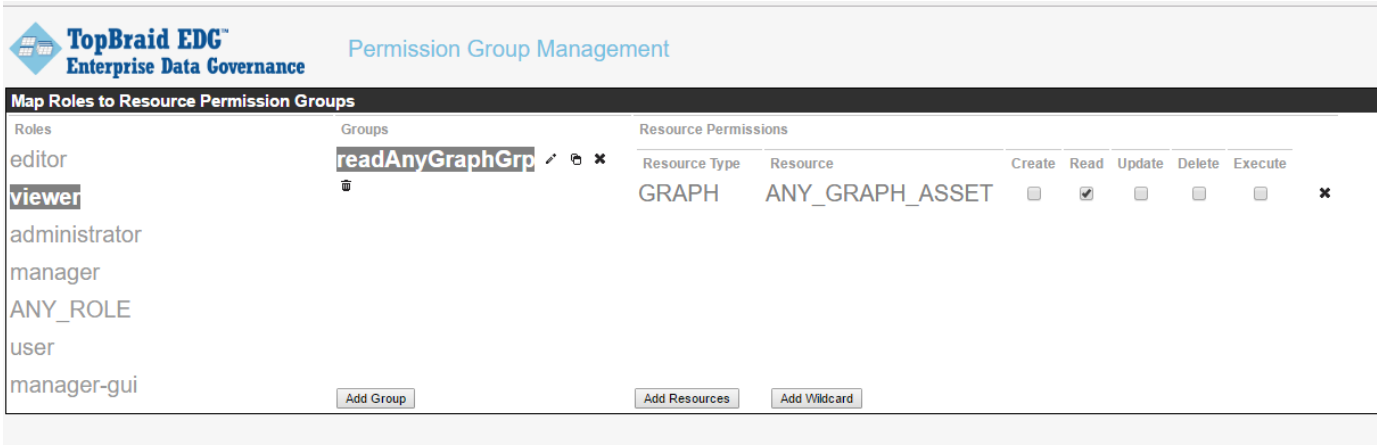
Select AdministratorGroup, it shows that it has all the CRUD-E permission for any resource.



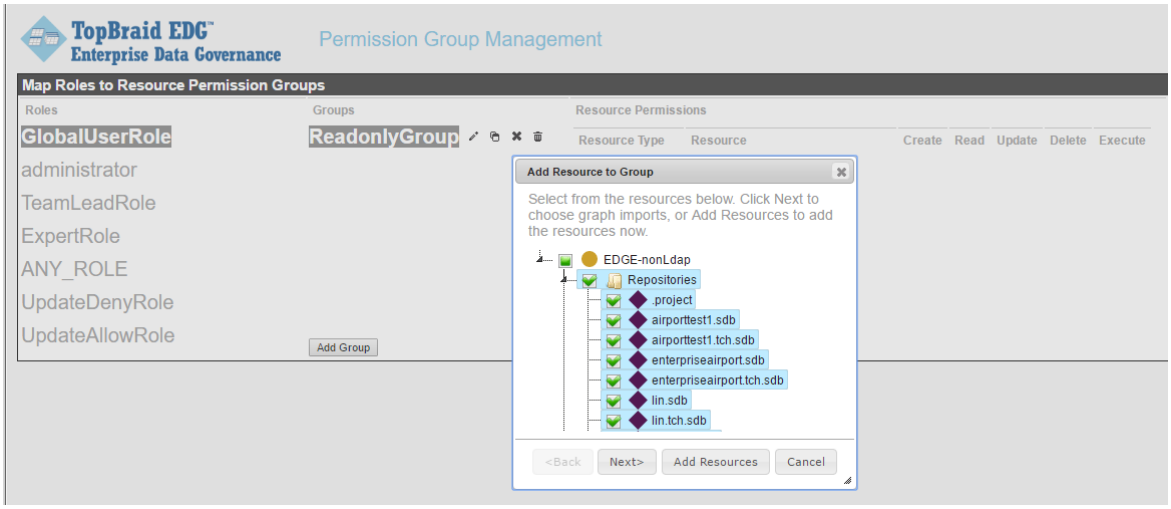
Example of adding groups to a role

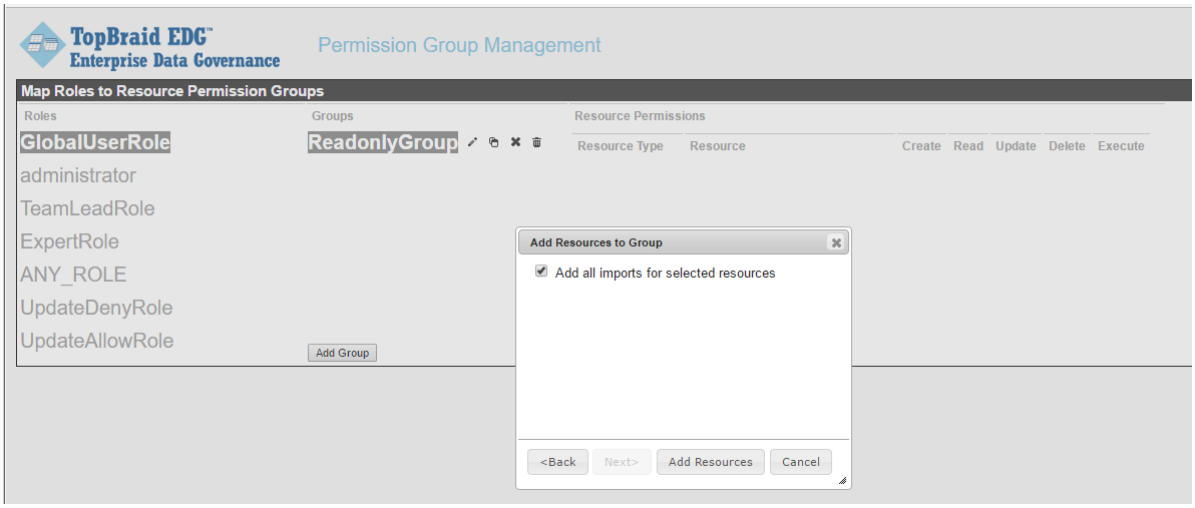
Use the 'GlobalUserRole' and add a group, resource, and project from the menu. Then adjust the permissions as needed.

Select 'GlobalUserRole' role on the left, Click on 'Add Group' button, then select the newly added group "readAnyGraphGrp", it shows the default set of resource permissions for this group, this only gives Read permission to all graph resources.

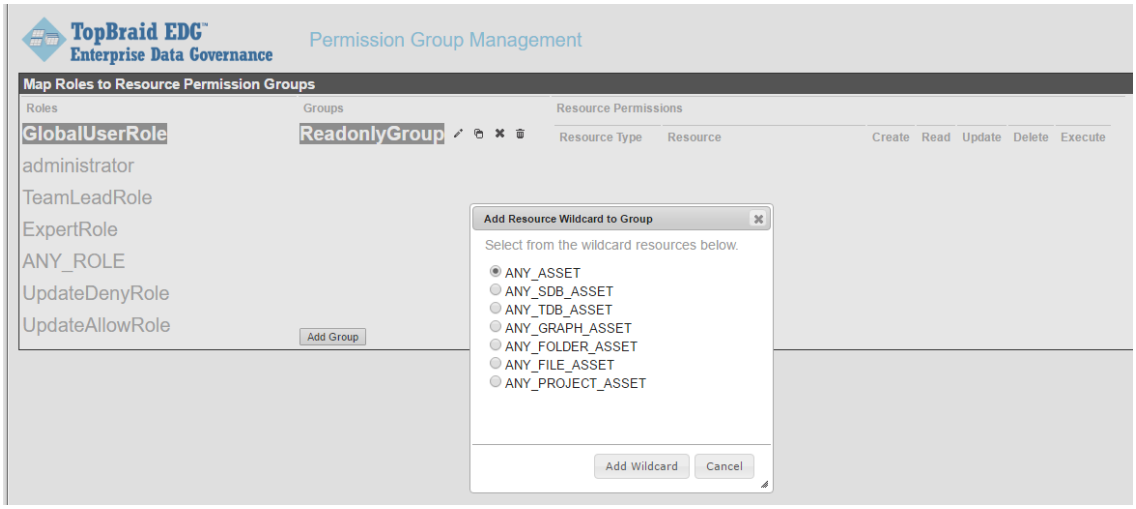


If you would like to have a specific set of resources permission, you can create a new group and start adding resources to the group. Click 'Add Group' and select 'New Group' to create a new group called it 'ReadonlyGroup'. Then click 'Add resources' for that group, select the resources from the tree. Click next to choose graph imports or 'Add resources' to the group without dealing with permission of the import.

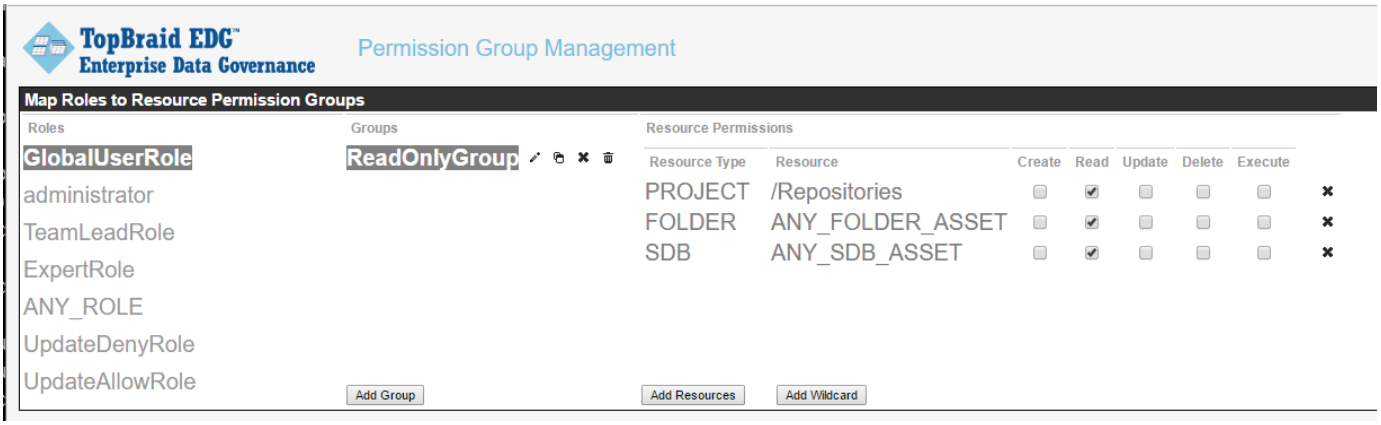




Add wildcard if needed:



Configure the CRUD-E permissions as needed:

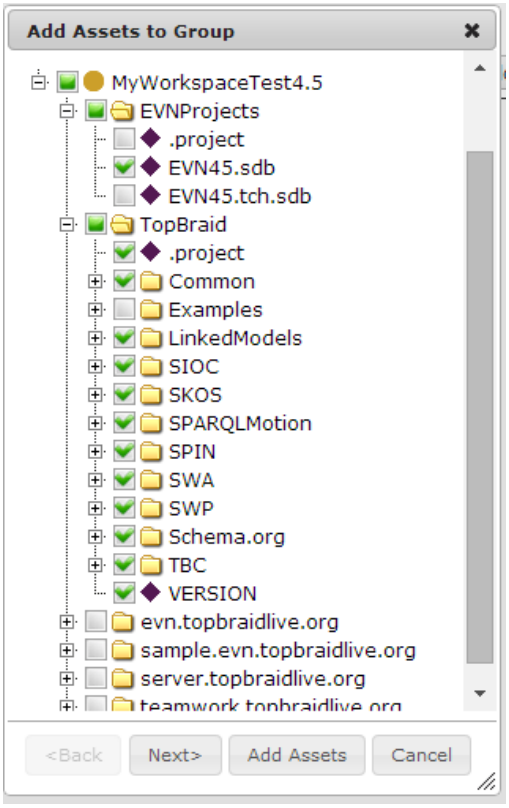


Resource Permissions

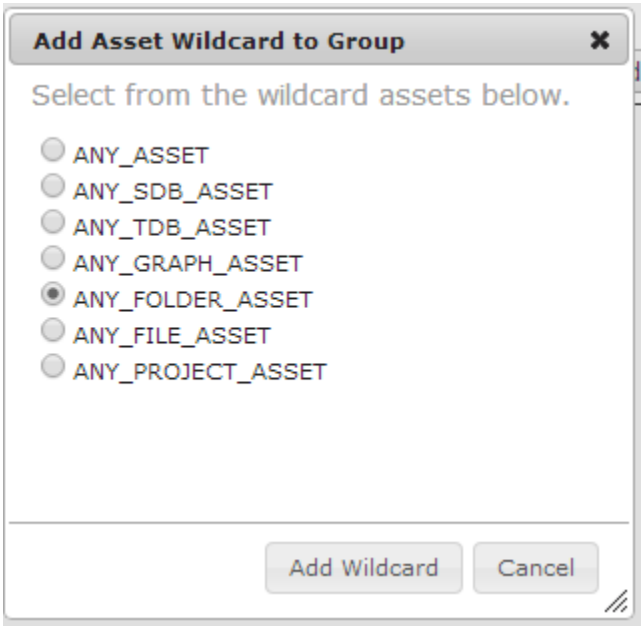
One or more resource definition is associated with each Group. The resource definition consists of a resource, either PROJECT (via the 'Add Resource' button) or ANY (via the 'Add Wildcard' button) and the CRUD+E access type definition. The choices are described in the following sections.

Resource Types

The two resource types are PROJECT and ANY. Clicking the 'Add Resources' button will bring up a window that shows a list of projects in the workspace, you can choose the individual projects (multi-select) or drill down the tree to select a specific file within a project.



Instead of selecting project resource, you can choose 'ANY' by clicking the 'Add Wildcard', select the radio button for a type of 'ANY' resource of your choice. Only one can be selected among this list



Definition of ANY Resource Types

The defined ANY resource types are as follows. These are used to allow administrators to define the different kinds of resources available in TopBraid Suite.

- **ANY_ASSET:** Any resource defined by TopBraid.
- **ANY_SDB_ASSET:** Any SDB data connector (.sdb file).
- **ANY_TDB_ASSET:** Any TDB data connector (.tdb file).
- **ANY_GRAPH_ASSET:** Any named graph in the TopBraid workspace. This is a superset of ANY_SDB_ASSET AND ANY_TDB_ASSET.
- **ANY_FOLDER_ASSET:** Any folder in the TopBraid workspace.
- **ANY_FILE_ASSET:** Any file that is not a graph, such a text, Excel, XML, etc.
- **ANY_PROJECT_ASSET:** Any project in the TopBraid workspace. This differs from the PROJECT resource type in that this refers to all Eclipse/Equinox project in the workspace.

Definition of Access Types (CRUD+E)

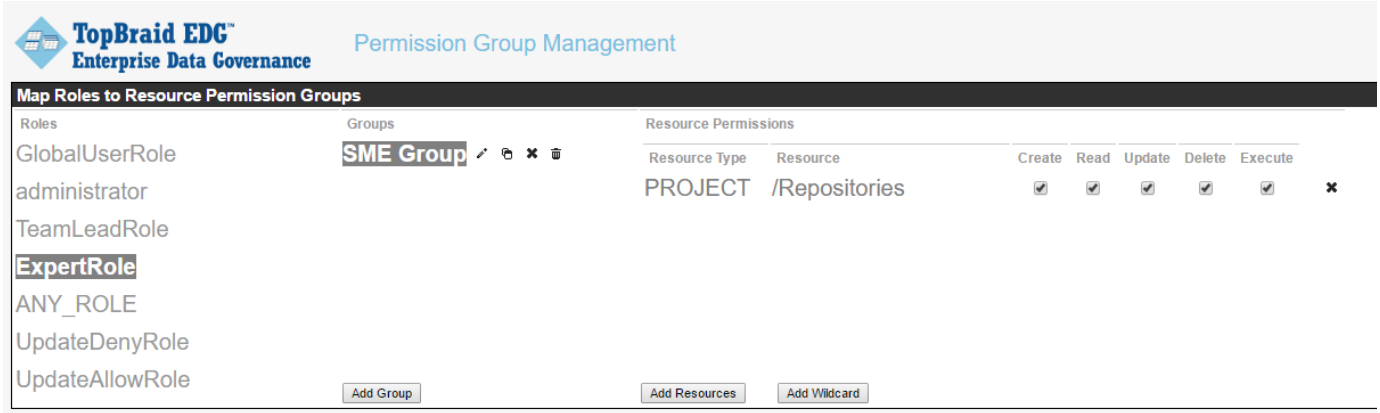
The access types are as follows:

- **Create:** Group members can create new resources.
- **Read:** Group members can read resources.
- **Update:** Group members can update/modify resources.
- **Delete:** Group members can delete resources.
- **Execute:** Group members can execute server-side scripts.

Suggested setup for TopBraid EVN

TopBraid EVN provides features that let users easily manage access to EVN asset collections (taxonomies, ontologies, tag sets, etc.) on a per collection basis. This is accomplished by assigning, in a context of a specific asset, the EVN asset-collection permissions *manager*, *editor*, and *viewer* to user id's or Tomcat Realms roles . These assignments can be set by the manager of each EVN asset collection.

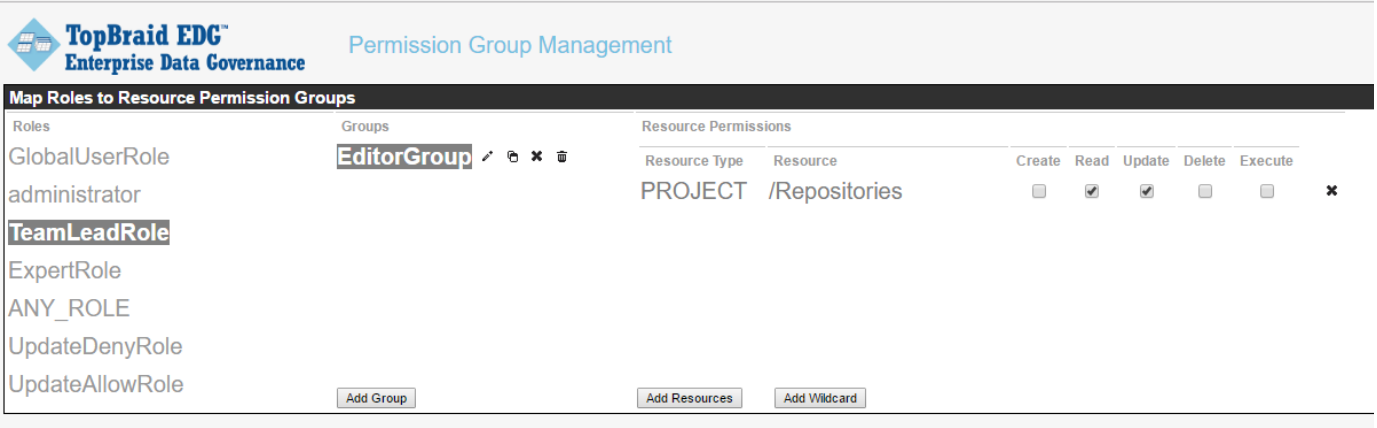
Given the use of EVN User Roles, the best practice is to define a small set of groups with access for the Eclipse/Equinox project that contains connectors to EVN data. One approach is to provide all EVN users (via their roles) with full CRUD+E access. This is depicted as follows, where the Eclipse/Equinox project is the default "Repositories". Anyone is of the role 'ExpertRole' belongs to 'SME Group' (subject matter expert), which has full permission in the Repositories project.

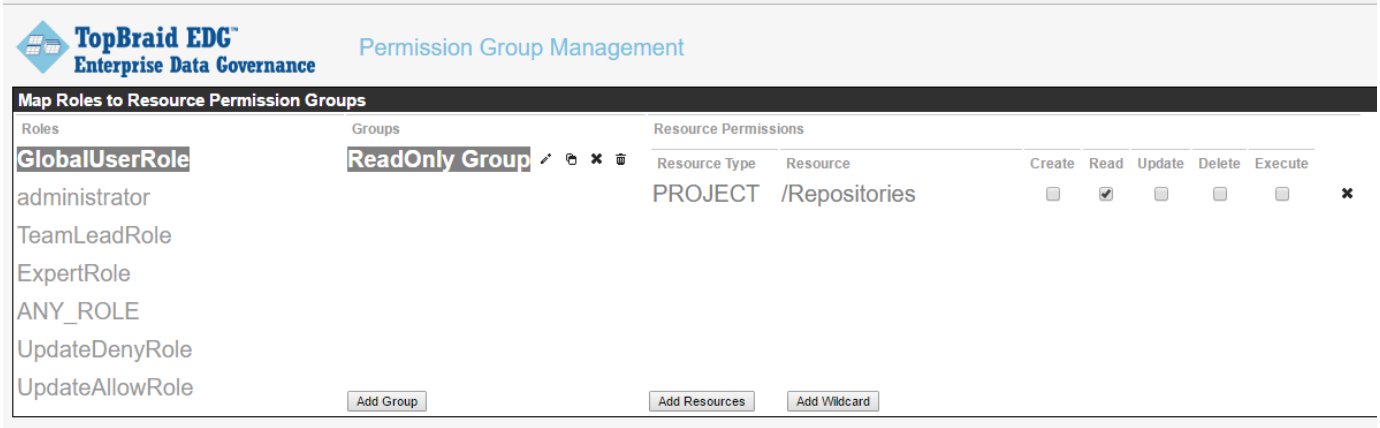


Another approach is to define access groups for Admin, general user (read/update/execute), and read-only user. Start by creating three groups, named "SME Group", "Editor Group", and "ReadOnly Group" in this example. Note the access types for each.

In this setup only users in 'ExpertRole' can create and delete in the 'Repositories' Projects with Read, Update and Execute rights as shown above. Users in the 'TeamLeadRole' will be able manage, edit, and view things in the 'Repositories' Projects, but not create or delete EVN vocabulary/asset . Depending on the User Roles assigned in the vocabulary/asset, any user in 'ExpertRole' and 'teamLeadRole' can be assigned 'manager', 'editor' or 'viewer' privileges in EVN User Roles. Users in the 'GlobalUserRole' can only read anything in the 'Repositories' projects. If a 'GlobalUserRole' user is assigned 'manager' or 'editor' EVN User Roles for a given vocabulary/asset, they are allowed to manage or edit such particular vocabulary. In other words, the vocabulary/asset manager assignment for a role in a given vocabulary/asset overrides the specification of such role set up by the system administrator in this permission group management page.

Users in multiple roles will be given the union of the assigned Group access rights.

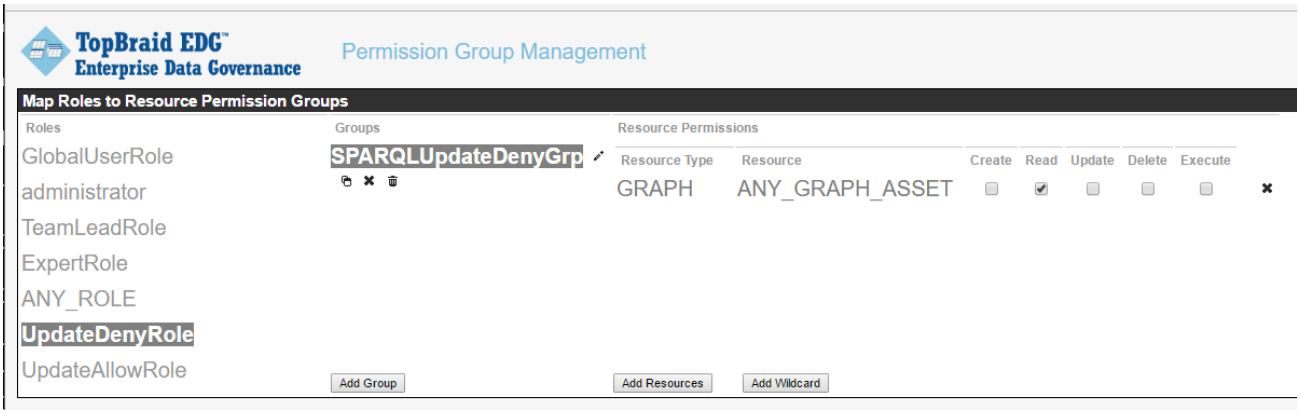




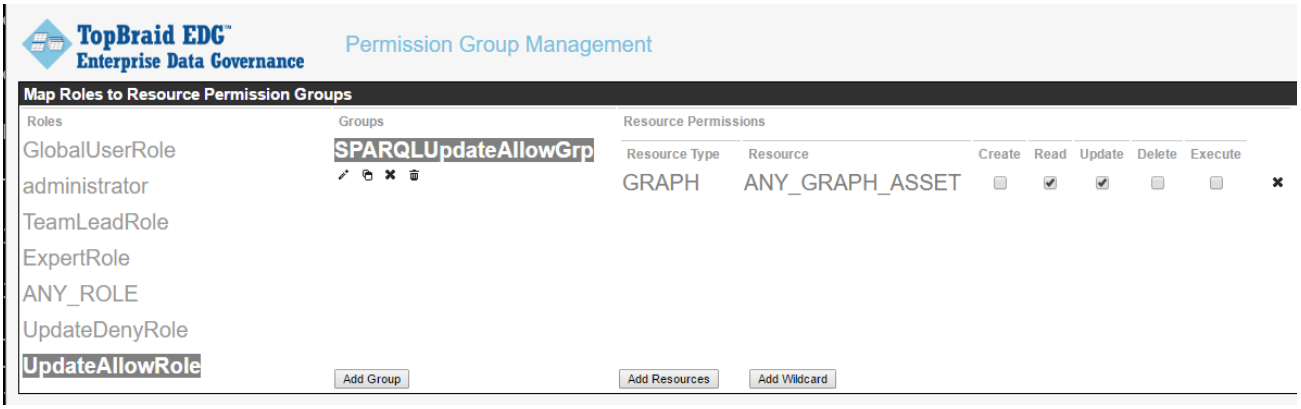
SPARQL Endpoint Update

TopBraid supports the SPARQL Endpoint update with two levels of security. First, the Server Configuration Parameter "Enable SPARQL updates" must be set to "true" from its default value (see Server Configuration Parameters). Secondly. the user must belong to a role that allows SPARQL Endpoint updates. In addition, roles can be defined that explicitly deny access to SPARQL Endpoint update:

- To block a roles from using a SPARQL endpoint to update graphs - assign those set of users a role and assign the SPARQLUpdateDenyGrp permission group to that role.



- To allow roles to use a SPARQL endpoint to update graphs - assign those set of users a role and assign the SPARQLUpdateAllowGrp permission group to that role.


TopBraid EDG
Enterprise Data Governance
Permission Group Management
Map Roles to Resource Permission Groups
Roles
GlobalUserRole
administrator
TeamLeadRole
ExpertRole
ANY_ROLE
UpdateDenyRole
UpdateAllowRole
Groups
SPARQLUpdateAllowGrp
Add Group
Resource Permissions
Resource Type
Resource
Create
Read
Update
Delete
Execute
GRAPH
ANY_GRAPH_ASSET
Add Resources
Add Wildcard