Access Control

Page Contents

Provide secure storage password

Enter here the *Master password* that EDG uses to encrypt its secure storage (e.g., for database passwords). This is an alternative to storing the Master password in plain text in the server's *web.xml* file.

Rights Management

Rights (group) management is the basic access control subsystem for a few items in EDG:

- Changing “Any_Role (all users) are administrators” to a specified tomcat role having administrator rights.
- Selecting the security role(s) that can create new asset collections by checking the Create box for that tomcat role.
- Making selected graphs OTHER THAN EDG asset collections publicly readable. This option is typically applied to files uploaded from TBC to the server.

This page DOES NOT control the read/write access for any asset collections created in EDG.

Rights management consists of two kinds of activities:

- defining *rights groups*, and
- assigning user *security roles* to various rights groups.

Each rights group represents specific access rights (i.e., **C**reate, **R**ead, **U**pdate, **D**elete and **E**xecute) on the group's selected workspace resources (or their generic "wildcard" types). For example, a file can be specified with CRUD access, whereas a SPARQLMotion script should have CRUD+E, and an exposed web service should only have E access. Users are then assigned to rights groups according to their *security roles*.

Prerequisite: Users' Security Roles

The users' side of rights management consists of knowing their security roles, which are configured during EDG's installation and initial setup. A user security role must:

1. be defined in a Tomcat/Realm, such as LDAP or `tomcat-users.xml`, and
2. it must appear in the permitted security roles setup of the TopBraid (which define entries for security-constraint tags in the application’s web.xml).

See Server Installation and Integration for details.

EDG also has one special, pre-defined (pseudo-) security role: *ANY_ROLE*, which automatically represents every user. This role can be used to assign access rights universally.

Defining Rights Groups

AdministratorGroup

EDG has a special, pre-defined rights group: *AdministratorGroup*, which conveys full access to all EDG resources (including asset collections in EDG).

The AdministratorGroup must always be assigned to at least one users security role that has at least one accessible login.

On initial EDG installation, the AdministratorGroup is assigned to ANY_ROLE. **This assignment should be moved** to one or more proper security roles as part of the initial application setup (by first assigning the AdministratorGroup to a proper role, then deleting it from ANY_ROLE).

Defining new groups

To define a new rights group: select an existing role > click **Add Group** > choose the **–New Group–** option > enter a name for the new group > click **Create Group**.

Rights groups cover one or more resources in the EDG's workspace, including projects (directories/folders) and various types of files. The selected group's workspace resources are listed in the *Resource Rights* section. Resources can be added or deleted, and each resource's access rights can be enabled or disabled. To add *particular* workspace resources, click the **Add Resources** button. To add *generic* resource types, click the **Add Wildcard** button. The defined *ANY_* resource types are as follows.

- **ANY_RESOURCE:** Any resource defined by TopBraid.
- **ANY_SDB_RESOURCE:** Any SDB data connector (.sdb file).
- **ANY_TDB_RESOURCE:** Any TDB data connector (.tdb file).
- **ANY_GRAPH_RESOURCE:** Any named graph in the TopBraid workspace. This is a superset of ANY_SDB_RESOURCE and ANY_TDB_RESOURCE.
- **ANY_FOLDER_RESOURCE:** Any folder in the TopBraid workspace.
- **ANY_FILE_RESOURCE:** Any file that is not a graph, such a text, Excel, XML, etc.
- **ANY_PROJECT_RESOURCE:** 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.

Then for each resource item, select which specific CRUD+E access rights are enabled or disabled for the group. 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.

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 contain **no** spaces - if they do, you will get an error trying to expand them. Please correct the source Project name and re-upload it with no spaces.*

Password Management

Users with privileges to view the Password Management page can add, delete, or edit the password entry in the secure storage. The "Add Password" button lets users add the password, and when the entry is selected, the user then can change the password for that entry or click the **x** to delete that entry.

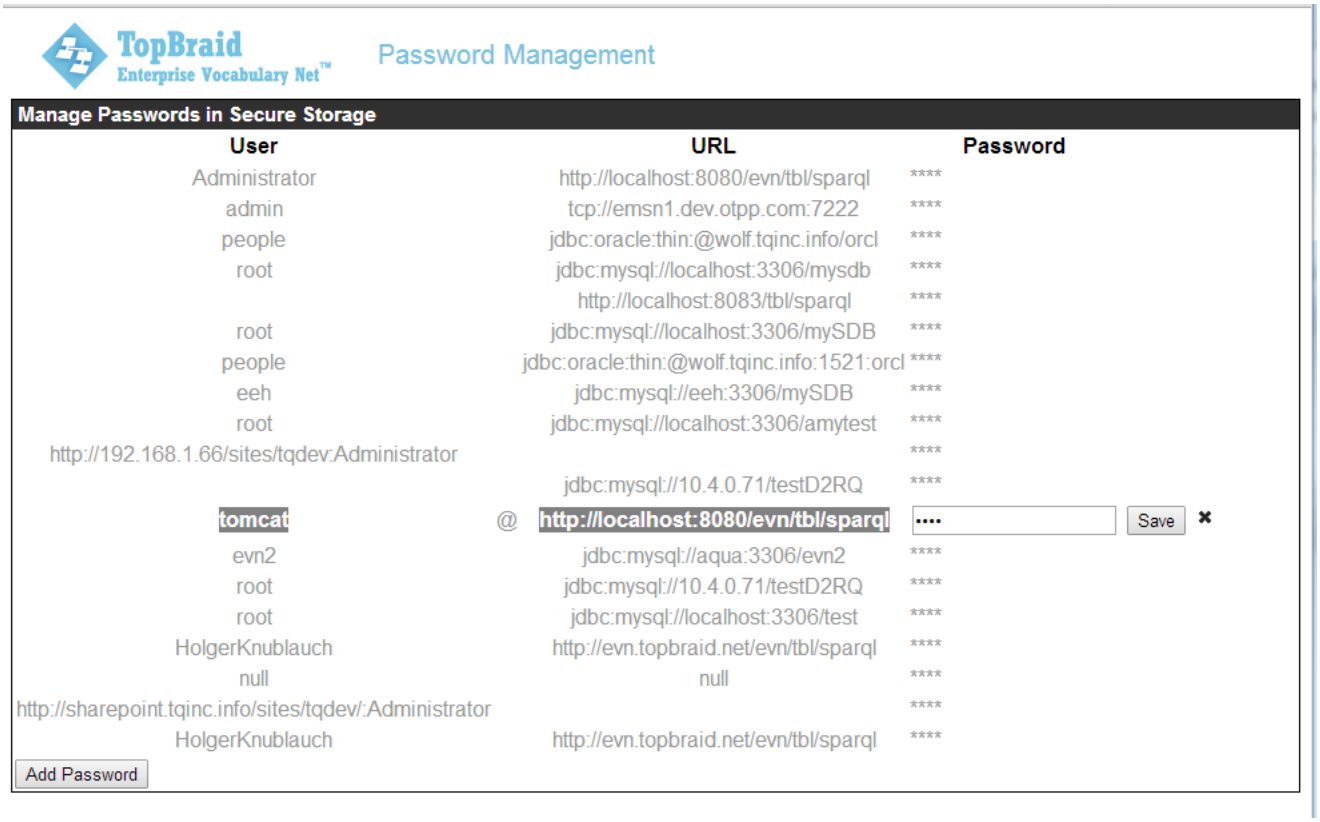
The Password Management page manages the contents of Equinox secure storage, which defines an encrypted file indexed by a URL and user id and storing a password encrypted by the secure storage password and the key. This means in particular that if the user id or URL changes for a given entry, the password must be re-entered using this page or any other sources for secure storage entries.

There are two sources for secure storage passwords:

1. Checking the "Send necessary connection credentials" in TopBraid Composer's **Export > Deploy project to TopBraid Live Server**. This sends the contents of the Composer user's local secure storage to the server's secure storage. This is necessary when one is

deploying a project from the IDE (Composer) that may contain passwords for connector files, SPARQLMotion scripts, etc. Note that to transfer the data form Composer's secure storage to the server's secure storage requires unencrypting Composer's secure storage and sending the content in plain text. For full security, use https when performing a deploy that includes "Send necessary connection credentials",

2. Using this page.



EDG Rights: Create for the Teamwork Repositories Project

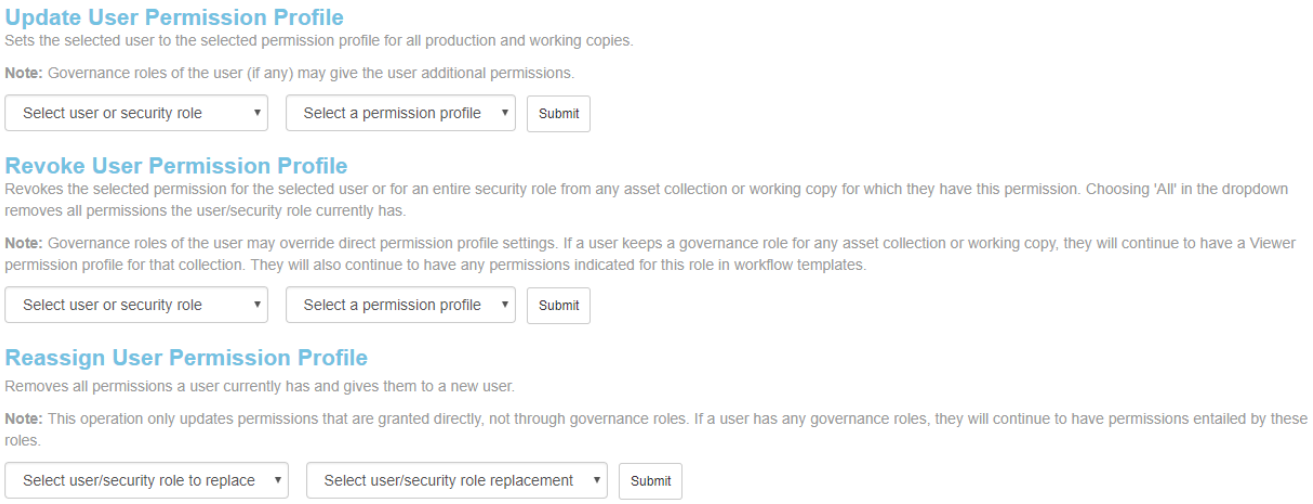
EDG has a *Teamwork* framework that controls access to asset collections via *permission profiles* (i.e., *viewer, editor,* and *manager*). It also has a Governance Model that uses *governance roles* to control access to the collections and their workflows via governance areas. (For an overview of access control in EDG, see Governance Model > Overview: Asset Collections and Governance.)

Both permission profiles and governance roles are largely separate from rights groups—*except* that for EDG users to *create* asset collections, they require the **`Create`** right on the EDG *Respositories project* (at least).

EDG Permissions Management

This view gives administrators global access to *permission profile* settings for current EDG asset collections. (For an overview of access control in EDG, see Governance Model > Overview: Asset Collections and Governance. For details on permission profiles for EDG asset collections, see Workflows > Collection Permission Profiles.) Administrators can assign or revoke either individual users or their security roles to **viewer**, **editor** or **manager** profiles for any or all collections, along with their working copies.

The first three settings let administrators (re-) assign or remove profiles for users on *all* collections:



click image to enlarge it

The sections below let you define or remove assignments specific to each collection:

In the following, the Administrator and Jane Smith have been assigned an editor role for the Enterprise Ontology vocabulary, and JimHarrison is being assigned a viewer role for the same vocabulary:

Note that roles are modular and thus can be assigned roles like users.