User Management

Overview

Documents the process for creating users, managing user application roles, and managing user project roles.

Authentication

The default security service implementation (SecurityServiceJpa) uses the IHTSDO user management system. Upon authentication, a REST call is made to the configured management service to validate the user and get some basic information. If authentication is successful, the map user information tracked by the application is updated to the latest state (including the user's name and email address). If there isn't a map user with that username yet in the system, one is added with a default VIEWER application role.

Thus, the sequence is something like this

- SecurityServiceJpa.authenticate is called with a username and password
- A call out is made to the IHTSDO user management system
    - e.g. https://usermanagement.ihtsdotools.org/security-web/query/
- Upon successful authentication, user information is returned, including the user's full name and email address
- If a map user with the corresponding username exists
    - The map user information is updated
- If a map user with the corresponding username DOES NOT exist
    - A new map user is created with the username, full name, and email address and a default VIEWER application role
- An authentication token is created and returned to the calling application for use validating subsequent mapping tool REST calls.

Configuration

The security service is configured by three properties in the config.properties file used by the running application.

- ihtsdo.security.activated

    - Indicates whether security is turned on or off
- ihtsdo.security.url=https://usermanagement.ihtsdotools.org/security-web/query/

    - The REST service URL to which an authentication call can be made
- ihtsdo.security.timeout=7200000

    - The timeout amount (in milliseconds) after which a user is automatically logged out and their authToken is invalidated.

Inactivated Authentication

If the "activated" flag is set to false, the behavior is a little different. In that case, the sequence is like this:

- SecurityServiceJpa.authenticate is called with a username and password
- Any password is accepted as legitimate for the username
- The system attempts to find a map user with that username, if one does not exist, authentication fails.
- If it finds that user, it creates and returns an authToken matching the username.

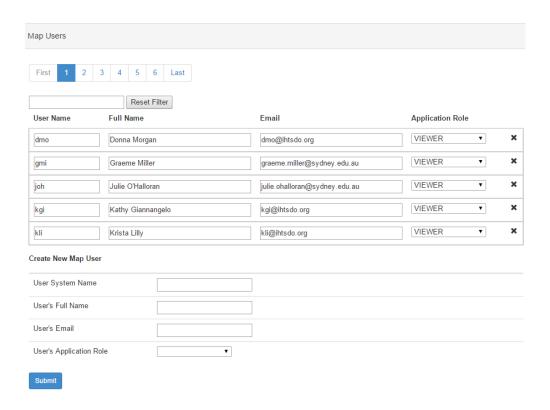Thus, in an "inactivated" system, users cannot be created simply by logging in.

Guest Authentication

The default security service also has special handling for the user "guest" which is authenticated by any password. The default installation of the system runs the "import.sql" file which creates the "guest" user in the map_users table. That means this user always exists and doesn't require authentication. The sequence of events is exactly the same for guest login as for when security is inactivated (NOTE: this is true for guest user even if security is activated).

Adding an Admin User via Webapp

An admin user must exist in order to perform top-level application administration activities (such as changing the application role of a user to ADMINISTRATOR). In a new system without an existing user with role ADMINISTRATOR, there is a mojo for creating an initial admin user. See Creating an Administrative User for more details.

Once you have a user with role ADMINISTRATOR, you can log into the application with that role and use the "Map Users" accordion on the "Application Administration" widget (on the adminstrator dashboard). From here, you can create new users and edit the application role of existing users.

Map Users

[   ] [Reset Filter]

User Name	Full Name	Email	Application Role	
dmo	Donna Morgan	dmo@ihtsdo.org	VIEWER ▼	✖
gmi	Graeme Miller	graeme.miller@sydney.edu.au	VIEWER ▼	✖
joh	Julie O'Halloran	julie.ohalloran@sydney.edu.au	VIEWER ▼	✖
kgi	Kathy Giannangelo	kgi@ihtsdo.org	VIEWER ▼	✖
kli	Krista Lilly	kli@ihtsdo.org	VIEWER ▼	✖

Create New Map User

User System Name	[ ]
User's Full Name	[ ]
User's Email	[ ]
User's Application Role	[▼]

[Submit]

Adding an Admin User Via Mojo

If no admin user exists, an admin user can be created using a mojo. To create the admin user, execute the following commands:

```
cd code/admin/loader
mvn clean install -PCreateMapAdmin -Drun.config=YOUR_CONFIG_VARIABLE -Dmap.user=DESIRED_USER_NAME
```

Executing this command will:

- Create a new map user will be created with the following default values. To edit these, edit the map user from the Application Administration widget.
    - System user name: DESIRED_USER_NAME
    - User's full name: DESIRED_USER_NAME
    - Email: Not set
    - Application Role: ADMINISTRATOR
- If no map projects currently exist, create a new map project named Blank Project with blank or default values.

After execution, log in as the specified user to edit existing projects or the newly created Blank Project, create additional projects, or perform other administrative tasks.
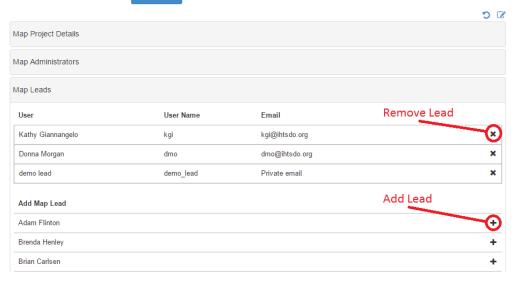
Adding Users and Setting Project Roles

WARNING: Do Not Assign Project Roles to ADMINISTRATOR Users

It is strongly recommended that you create an ADMINISTRATOR user for administration and have separate users for lead and specialist roles on projects. Project roles override application roles when deciding which dashboard to show for a user. Thus, an ADMINISTRATOR user who is a lead on a certain project will see the lead dashboard instead of the admin dashboard when the focus project is set to that project.

Project roles for existing map users can be set by lead or admin users via the "Project Details" page for a specified project.

- Log in as a lead or admin user
- Choose the focus project you want to edit specialist/lead users for
- Go to the "Project Details" page
- Click the "enable edit mode" icon at the top of the table to turn on edit mode
- Navigate to the "Map Specialists" (or "Map Leads") accordion in the project details widget and open it.
- You will see users currently marked as specialists (or leads).
- Click the X icons to remove users from this role
- Click the + icons to add users to this role

SNOMED to ICD10 [Map Records]

Map Project Details

Map Administrators

Map Leads

User	User Name	Email	
Kathy Giannangelo	kgi	kgi@ihtsdo.org	**Remove Lead** ✖
Donna Morgan	dmo	dmo@ihtsdo.org	✖
demo lead	demo_lead	Private email	✖

Add Map Lead

		Add Lead
Adam Flinton		➕
Brenda Henley		✚
Brian Carlsen		✚

References/Links

- See tour related to this: General Training 004