Data authorization

Summary: This section describes how to configure data authorization in the CAST dashboards.

Introduction

An **Authorization** defines permission to access and "consume the data" in **a specific Application** or **group of Applications** via the CAST dashboards. If permission is not granted, or a "**restriction**" is used, then any information related to this Application will be not accessible: application properties such as name, technologies or grades and measures, etc. Therefore, an Authorization must be defined before a user/group of users can access a specific application:

- Data authorization can ONLY be configured once a snapshot has been generated and the relevant data is present in the CAST AIP schema.
- Users are not automatically granted any data authorization, therefore authorizations must be granted before the dashboards can be used. Note however, that a user with the **ADMIN role** will automatically be granted authorization to access **all Applications**.
- If a user is not authorized to access any data at all, upon login, a message will be displayed explaining that the user is not authorized to access any data and further use of the dashboard is prevented. It is also possible to modify the message that is displayed, see **Modifying login error messages**).
- Data authorization functions for **all authentication modes:**
  - If you are using **Default Authentication mode**, the users you use to grant authorizations must already be defined in the **users.properties** file
  - If you are using **Standard LDAP** or **SAML modes**:
    - the users and groups you use to grant authorizations must already exist in your LDAP/SAML environment.
    - **Common Names** must be defined (not Distinguished Names) in the configuration files when using Dashboards 1.x
- Data authorization can be configured for **Dashboard schemas** and for **Measurement schemas**.
- If the username contains special characters (non US-ANSI characters) such as **é,è,à,ç,ù** etc., you must ensure that your text editor saves the **authorization.xml/license.xml** file with utf-8 encoding.

Authorizations/restrictions when using the combined war/zip files

When you are using the the **combined Health/Engineering WAR/ZIP files**, please remember that data authorization is **common** to the Measurement schema (Health Dashboard) and Dashboard schema (Engineering Dashboard) defined in the dashboard connection properties. Therefore if you authorize "UserA" to view Application "B", then this is true for both dashboards delivered in the same WAR/ZIP file. The **exception** is when you are using a restricted license where authorizations for the Engineering Dashboard must be defined in **license.xml** - therefore authorizations for the Health Dashboard can differ to those defined for the Engineering Dashboard.

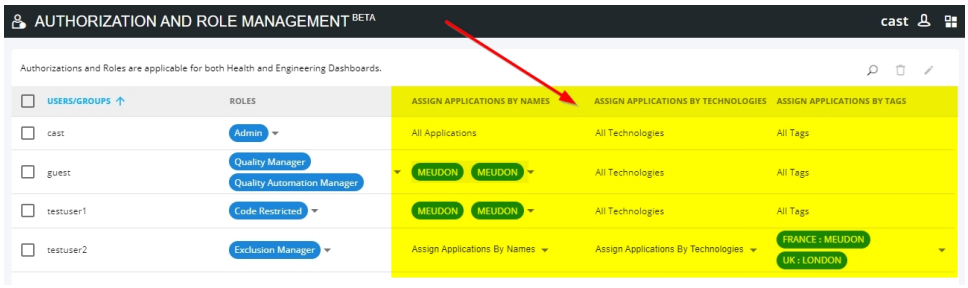
When you are using the combined WAR/ZIP file, authorizations/restrictions based only on **Tags** and **Categories** created solely for Measurement schemas (Tag and Categories are features that are not available for Dashboard schemas) WILL also be applied in the Engineering Dashboard for applications that exist in both schemas.

How is data authorization managed?

Data authorization is managed in different ways depending on the Dashboard release you are using:

2.x

Data authorization is managed using a graphical user interface. See **Data authorization - 2.x and above**:



> Note that this user interface is also used to assign **User roles - 2.x and above**.

1.x

Data authorization is managed using a configuration file called **authorizations.xml (and license.xml for those using a RESTRICTED license)**. See **Data authorization - 1.x**.

```
<root>
   <authorization user="guest" application="Billing platforms" adgDatabase="demo_central"/>
</root>
```