CAST-AED - Configuring data authorization

On this page:

Target audience:

CAST AI Administrators

Summary: This section describes how to configure data authorization in the **CAST Application Engineering Dashboard**.

Introduction

An **Authorization** defines permission to access and "consume the data" in a specific Application in the CAST Application Engineering Dashboard. If permission is not granted 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.

Notes:

- Data authorization can ONLY be configured once a snapshot has been generated in a Dashboard Service connected to the CAST Application Engineering Dashboard
- By default, no users are granted **all Applications** access
- A user with the ROLE_ADMIN role will automatically be granted authorization to access **all Applications**
- Users (whether static-list or Active Directory) are not automatically granted data authorization - an error will therefore be displayed when a user attempts to log in because the user is not authorised to access any data.
- Authorizations function for both static-list and Active Directory authentication mode
- 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 file** with utf-8 encoding.
- 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 CAST Application Engineering Dashboard is prevented - this is described in CAST Application Engineering Dashboard - CAST AED under **Logging in to the CAST Application Engineering Dashboard**. It is also possible to modify the message that is displayed, see CAST-AAD-AED - Modifying login error messages.
- When a RESTRICTED **license key** for accessing the CAST Dashboard Service is in use, all authorizations defined in **authorizations.xml** are ignored. Please see CAST-AED-RESTAPI - Dashboard Service license key configuration for more information about this.

Authorizations are defined in the following file:

```
%CATALINA_HOME%\webapps\CAST-AED\WEB-INF\authorizations.xml
```

Each line of the **authorizations.xml** file defines a permission to access an application or a set of applications. These lines are cumulative, therefore several lines can be applied to one single user or group, in which case, this user or group will have access to the all specified applications. The syntax in use is as follows:

User scope, defined by the following attributes:

- user
- group
- allUsers="true"

Content scope, defined by the following attributes:

- application, adgDatabase
- applicationPattern, adgDatabasePattern
- allApplications="true"

Authorizations when using the combined CAST-AAD-AED.war file

When you are using the CAST Application Engineering Dashboard via the combined CAST-AAD-AED.war file (as described in Installing and configuring the CAST Application Engineering Dashboard), please remember that data authorization is **common** to both Dashboards. Therefore if you authorize "UserA" to view Application "B" only via the **authorizations.xml file**, then this is true for both Dashboards.

> Note that authorizations based only on **Tags**, **Categories** and **Technologies** created solely for the CAST Application Analytics Dashboard (Tags, Categories and Technologies are a feature that is not available in the CAST Application Engineering Dashboard) WILL be applied in the CAST Application Engineering Dashboard when using the combined war file. See CAST-AAD - Configuring data authorization for more information about these authorizations.

Authorize a user to access an application

You can define authorization to a single application by specifying its name AND the name of the CAST Dashboard Service database/schema in which the snapshot results for the Application are stored. For example, this line grants the "guest" user access to the "Billing platforms" application stored in the "demo_800_central" database:

```
<root>
   <authorization user="guest" application="Billing platforms" adgDatabase="demo_800_central"/>
</root>
```

> Please note that the **adgDatabase** attribute is **case sensitive**. Therefore you must ensure that the name of the CAST Dashboard Service database/schema exactly matches the name defined in your RDBMS (whether CSS or Oracle/Microsoft SQL Server).

Authorize a user to access applications matching a pattern

You can authorize a user to access certain Applications based on regular expression pattern matching. With the following definition, the user "guest" will be authorized to access applications where the host CAST Dashboard Service is equal to "demo_800_central" or "demo_801_central" or "demo_802_central" or "demo_803_central" :

```
<root>
   <authorization user="guest" applicationPattern=".+" adgDatabasePattern="demo_80[0-3]_central"/>
</root>
```

> Note that:
>
> - pattern matching can only be applied to Applications (applicationPattern) and CAST Dashboard Services (adgDatabasePattern) - the two MUST always be applied together to distinguish Applications.
> - the **adgDatabasePattern** attribute is **case sensitive**. Therefore you must ensure that pattern of the CAST Dashboard Service database/schemas matches the case used in the database/schema names defined in your RDBMS (whether CSS or Oracle/Microsoft SQL Server).

Authorize a user to access all applications

A user can be authorized to consume all applications. This is the case for the default configuration of user "James".

```
<root>
   <authorization user="James" allApplications="true"/>
</root>
```

Authorizations are additive, therefore this authorization discards all other authorizations.

Authorize access for a group of users

In **each of the above use cases**, we can specify a **group** name (whether in Static List or Active Directory mode) in place of a **user** name. If Active Directory mode is being used, the group name must be specified using the full ***Distinguished Name*** **(DN)** of the group. Some possible examples are given below:

```
<root>
        <!-- authorize a static-list group to access all applications -->
        <authorization group="demo" allApplications="true"/>

        <!-- authorize a static-list group to access a specific application -->
        <authorization group="demo" application="Billing platforms" adgDatabase="demo_801_central"/>

        <!-- authorize an LDAP group to access all applications -->
        <authorization group="CN=corporate.products.dev-dashboard.aip,OU=GROUPS,OU=FR,DC=corp,DC=castsoftware,
DC=com" allApplications="true"/>

        <!-- authorize an LDAP group to access a specific application -->
        <authorization group="CN=corporate.products.dev-dashboard.aip,OU=GROUPS,OU=FR,DC=corp,DC=castsoftware,
DC=com" application="Billing platforms" adgDatabase="demo_801_central"/>
</root>
```

Authorize access for all users

It is possible to authorize access to **a single Application** or to **all Applications** for **all users** (whether in Static List or Active Directory mode) - users means all authenticated users:

For example, the following statement will allow **all users** to access data from the "**Financial**" application located in the "**demo_central**" Dashboard Service:

```
<authorization allUsers="true" application="Financial" adgDatabase="demo_central"/>
```

For example, the following statement will allow **all users** to access results from **all applications**:

```
<authorization allUsers="true" allApplications="true "/>
```