

2.1

- [Content matrix](#)
 - [User roles and data authorizations management interface - new in 2.1.x](#)
- [2.1.0-funcnel](#)
 - [New Features](#)
 - [Feature Improvements](#)
 - [Known Issues](#)

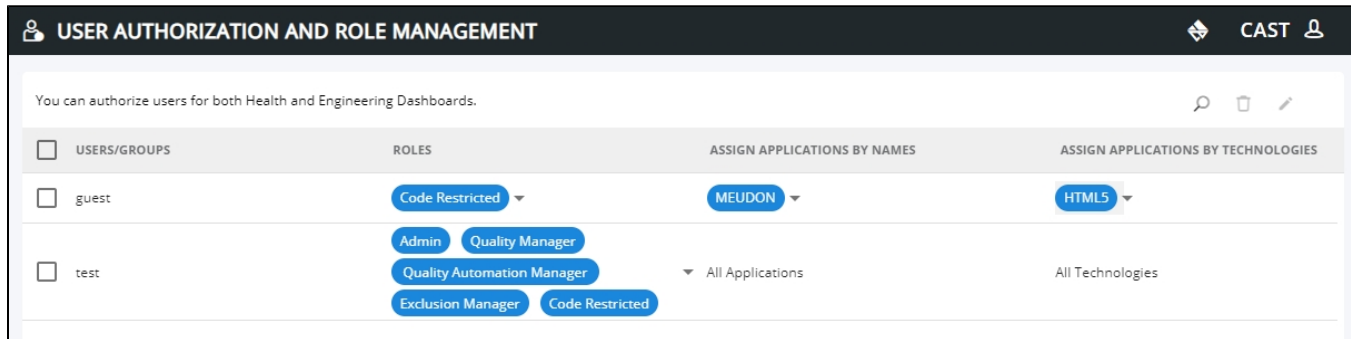
Content matrix

Version	Summary of content	Comments
2.1.0-funcnel	<ul style="list-style-type: none">• A graphical user interface has been implemented for managing the assignment of role and data authorizations to users and groups of users.• In advanced search, six new filter criteria (Business Criteria Name, Technical Criteria Name, Technology Name, Module Name, Weight, Critical value) are added as columns in exported excel reports.	<p>Can be used with:</p> <ul style="list-style-type: none">• 8.3.3

User roles and data authorizations management interface - new in 2.1.x

A **graphical user interface** has been implemented for managing the assignment of **role and data authorizations** to users and groups of users. This interface replaces the existing mechanism provided by the **roles.xml** and the **authorizations.xml** files. You can find out more in:

- [User roles](#) and [User roles - 2.x and above](#)
- [Data authorization](#) and [Data authorization - 2.x and above](#)



Some things to be aware of:

- This feature is in **beta** and **MUST NOT be used** if you have re-used an existing **authorizations.xml** file with the new deployment and this file contains authorizations defining specific "restrictions" or which define "application name patterns". In this case, the user interface must not be used and instead authorizations and roles must be updated using the REST API (see `/server/authorizations` and `/server/roles` web services).
- This new management interface relies on a **new schema hosted on a CAST Storage Service/PostgreSQL instance** to store the roles/data authorizations. This schema is called **cast_dashboards** by default and will be created on first startup of the web application. You will need to specifically configure a connection in the **application.properties** file to a CAST Storage Service/PostgreSQL instance which will be used to host the schema. This instance does not need to be the same as used for your AIP schemas (Dashboard/Measure schemas), however, the required schema is small and therefore CAST recommends using an existing CAST Storage Service/PostgreSQL instance to host it. The schema is created automatically when you start up your Dashboard deployment if it does not already exist. You can find out more information in Step 6 and 8 and in the following documentation:
 - [Deploy CAST Security Dashboard using WAR file#step6Step6-Configureroles](#)
 - [Deploy CAST Security Dashboard using WAR file#step9Step9-Configuredataauthorization](#)
- The **cast_dashboards** schema can be re-used across multiple dashboard deployments if your roles/authorization requirements are the same for all deployed dashboards
- If the **cast_dashboards** schema already exists on the referenced CAST Storage Service/PostgreSQL instance, it will not be recreated and any roles/authorizations defined in it will be re-used
- When using a **combined** Health and Engineering Dashboard deployment, the **cast_dashboards** schema and all roles and authorizations defined in it are valid for both dashboards
- You can use an alternative name for the **cast_dashboards** schema, for example if you are deploying multiple standalone dashboards but require different roles/authorizations assignments in each dashboard. See [Changing the name of the cast_dashboards schema](#).
- If you are using a **RESTRICTED license key** for access to the Dashboard schema (see [Data authorization - 2.x and above](#) and also [Dashboard Service license key configuration](#)):
 - AND a **standalone Engineering Dashboard** any authorizations must still be defined in the **license.xml** file.

- AND a **combined Engineering/Health Dashboard**, any authorizations for the Engineering Dashboard must still be defined in the **license.xml file** and any authorizations for the Health Dashboard must be defined in the new management interface
- Authorizations for **tags/categories** and **restrictions** are not supported in the new management interface
- If you are moving from a **previous 1.x or 2.0 release** (see [Standalone Dashboard upgrade](#)) and have a set of roles/authorizations you wish to retain, you have two choices:
 - You can provide your **roles.xml and/or authorizations.xml** file and on first start-up of the web application the role assignments will be **automatically transferred into the management interface**. The **roles.xml/authorizations.xml file will then be ignored** on any subsequent web application startup and all changes from then on must be performed using the graphical interface.
 - You can assign the **roles from scratch** using the graphical interface.
- Any changes made in the interface to assigned roles are only taken into account when the **user logs out and logs back in again**. Data authorizations are effective immediately.

2.1.0-funcrel

New Features

Summary	Details
UI - User role and data authorization management interface	A graphical user interface has been implemented for managing the assigning of role and data authorizations to users and groups of users. This interface replaces the existing mechanism provided by the roles.xml and the authorizations.xml files. See https://doc.castsoftware.com/display/DASHBOARDS/2.1#id-2.1-Userrolesanddataauthorizationsmanagementinterface-newin2.1.x for a summary of the changes and impacts.

Feature Improvements

Summary	Details
Advanced search - Need all filter criteria as columns in exported reports	In Advance search export report (six more columns) more details are added. The newly added columns are - Business Criteria Name, Technical Criteria Name, Technology Name, Module Name, Weight, Critical.

Known Issues

Internal Id	Details
DASHBO ARDS-00000	The new roles and authorizations management interface does not currently function in Microsoft Edge or Internet Explorer browsers.
DASHBO ARDS-00000	Restrictions are not currently supported in the new roles and authorizations management interface, however, if you provide an existing authorizations.xml file that defines restrictions, these will be taken into account when you first startup the web application but the restrictions will not be visible in the user interface. subsequently, if you need to modify these restrictions, you will need to use a RestAPI query. CAST intends to change this behavior in a future release.