User roles

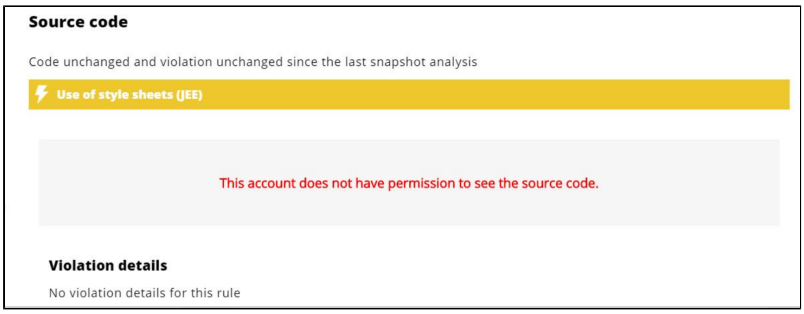
Summary: This section describes how to configure **roles** for users.

Introduction

Each dashboard has a variety of roles available that can be granted to **users** and **groups of users**. The purpose of roles is to grant additional permissions for specific situations and features.

What roles are available?

Role	Health Dashboard	Engineering / Security Dashboard	RESTAPI	Notes
ADMIN	✓	✓	✓	The **ADMIN** role provides permission to execute the following actions: **Health Dashboard** • **reload** the dashboard memory (see **Reload the cache**). • **create, update, delete** new **categories**, and **tags** with the **tags.html** administration page (see **Health Dashboard tag and** • **add** or **remove** applications to/from **tag assignments** with the **tags.html** administration page (see **Health Dashboard tag** • Ability to list **all applications** both for **tag assignment** or **access to applications** **Engineering Dashboard** • **reload the dashboard memory** (see **Reload the cache**). A user with the role **ADMIN** cannot interact with the Action Plan / Exclusion list / Education list - this requires the **QUAL** **QUALITY_AUTOMATION_MANAGER** roles (see below). **All dashboards** In addition, a user with the **ADMIN** role: • will automatically be granted authorization to access **all Applications** (allApplications authorization - see **Data authorizatio** • does not require a **license key** to access the data in the CAST Dashboard Service (**not applicable to Health Dashboard**) **configuration** • will gain admin specific options via the username button • will get **Check for update** option in the user profile drop down. It performs a check to see whether the current Dashboard is See: **Engineering Dashboard - GUI** You should use this role with caution!
QUALITY_MANAGER	✗	✓	✗	The **QUALITY_MANAGER** role provides permission to **add** and **remove** objects from the **Action Plan** and to use the **Engineerir** **Recommendation** feature. A user granted this role ALSO requires additional authorization to access Applications data - they will not configured - see **Data authorization**.
EXCLUSION_MANAGER	✗	✓	✗	The **EXCLUSION_MANAGER** role provides permission to **add** and **remove** objects from the **Exclusion list**. A user granted this r access Applications data - they will not be permitted to login if an authroization is not configured - see **Data authorization**.
QUALITY_AUTOMATION_MANAGER	✗	✓	✗	The **QUALITY_AUTOMATION_MANAGER** role provides permission to **add** and **remove** objects from the **Education list**. A user authorization to access Applications data - they will not be permitted to login if an authroization is not configured - see **Data autho**

CODE_RESTRICTED	✗	✓	✓	The **CODE_RESTRICTED** role prevents users from viewing source code in the Engineering Dashboard. When enabled, a messag when an attempt is made to view the source code of a violation: *Click to enlarge*   • This role is available in 1.11.0. • A user granted this role ALSO requires additional authorization to access Applications data - they will not be perm configured - see **Data authorization**.
NO_ROLE	✓	✓	✓	The **NO_ROLE** role is a "read-only" role - it does not grant any permissions. A user granted this role ALSO requires additional aut will not be permitted to login if an authorization is not configured - see **Data authorization**.

How are roles managed?

Roles are managed in different ways depending on the Dashboard release you are using:

2.x	Roles are managed using a graphical user interface. See **User roles - 2.x and above**:  Note that this user interface is also used to assign **Data authorization - 2.x and above**.

1.x	Roles are managed using a configuration file called **roles.xml**. See **User roles - 1.x**.
	
	`<root>`
	`  <role-assignment user="Bill" role="ADMIN"/>`
	`</root>`