Admin Center - Roles panel

ⓘ **Summary:** this page describes how to manage roles and their application authorities/resource permissions.

⚠ A user with the **ADMIN or SUPER ADMIN** role is required.

Introduction

The Roles panel enables you to manage the roles that can be granted to your users/groups (via the **Admin Center - Users panel**). All users MUST be granted a role (either directly to the user or to a group the user is a member of) before the user will be able to access application data or interact with CAST Imaging features.

CAST Imaging provides **four default roles out of the box** (see below) **for each tenant** and these can be supplemented with additional custom roles as required. Roles do two things:

- grant access to **application data** (either the role can access a single application, multiple applications or all applications):
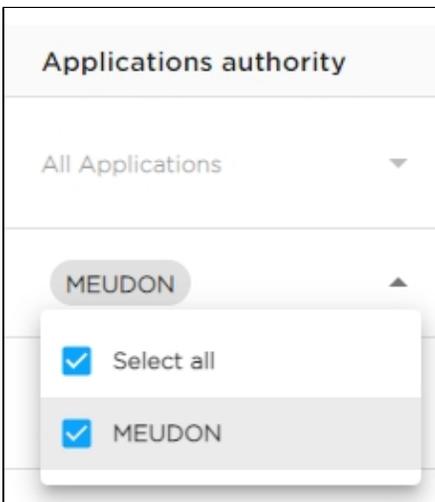
- grant varying degrees of access to **features within CAST Imaging** - this is known as "**resource permissions**". These resource permissions are granted using **READ, CREATE, UPDATE, DELETE** options. In the following example, a role grants READ and CREATE permissions on the **Document-It** resource (see **User Guide - Using the Document-It feature**). This means that a user assigned this role:
    - can READ existing Document-It items added to a view
    - can CREATE new Document-It items in a view
    - cannot UPDATE existing Document-It items in a view
    - cannot DELETE existing Document-It items in a view

A role can include **a mix of the two access type permissions** (application data and resource permissions), or it can include just one type (either application data or resource permissions) - in this latter case, multiple roles should be assigned to allow the user/group to interact correctly.

Default roles

Out of the box in a brand new installation of CAST Imaging, the following roles are made available in order of priority

SUPER ADMIN	The **SUPER ADMIN** role provides permission to execute the following actions in the **Admin Center** across all tenants: • Manage the import of applications - see **Admin Center - Application management panel** • Manage existing default roles and create/manage new custom roles (current documentation page) • Assign/revoke roles to users/groups - see **Admin Center - Users panel** • Manage app to app dependencies - see **Admin Center - Application to Application Dependencies management** • Manage preferences - see **Configuring display preferences** • Manage the multi tenant feature - see **Admin Center - Multi tenant panel** In addition: • Users and members of groups with the SUPER ADMIN role can access **all Application data** in CAST Imaging across all tenants • Users and members of groups with the SUPER ADMIN role have full resource permissions on all CAST Imaging features • this role is not specific to a single tenant, instead it is intended to be used as a "global administrator" with complete jurisdiction acros ⚠️ • The first user to log in to CAST Imaging following a fresh installation will receive the SUPER ADMIN as described in **First lo super admin**. • You should use this role with caution!
ADMIN	The **ADMIN** role is identical to the **SUPER ADMIN** except that: • this role cannot manage the multi tenant feature - see **Admin Center - Multi tenant panel** • this role is specific to each tenant - in other words it is the "SUPER ADMIN" role on a per tenant basis • if there is only one tenant in existence and the multi tenant feature is not used, then this role has identical permissions to SUPER AD ⚠️ You should use this role with caution!

ARCHITECT	The **ARCHITECT** role is intended to be granted to users/groups that do not require Admin Center access but require more access than s

This role does not grant any application access permissions therefore you will need to specify these manually
this role is specific to each tenant
the default set of resource permissions is as follows:

Click to enlarge

> ☐ **Admin Resources**   `Resource`

∨ ☑ **App to App Dependencies**   `Resource`

   ☑ READ   `Permission`

∨ ☑ **Custom Object Types**   `Resource`

   ☑ READ   ☑ UPDATE   ☐ DELETE   ☑ CREATE   `Permission`

∨ ☑ **Custom View**   `Resource`

   ☑ CREATE   ☑ READ   ☐ DELETE   ☐ UPDATE   `Permission`

∨ ☑ **Cypher Search**   `Resource`

   ☑ READ   ☐ CREATE   `Permission`

∨ ☑ **Document-It**   `Resource`

   ☐ DELETE   ☑ CREATE   ☑ UPDATE   ☑ READ   `Permission`

∨ ☑ **Services View**   `Resource`

   ☑ READ   `Permission`

∨ ☑ **Sourcecode Viewer**   `Resource`

   ☑ READ   `Permission`

∨ ☑ **Tags**   `Resource`

   ☐ DELETE   ☑ UPDATE   ☑ READ   ☑ CREATE   `Permission` |

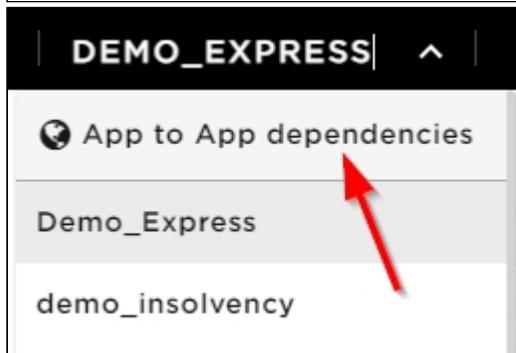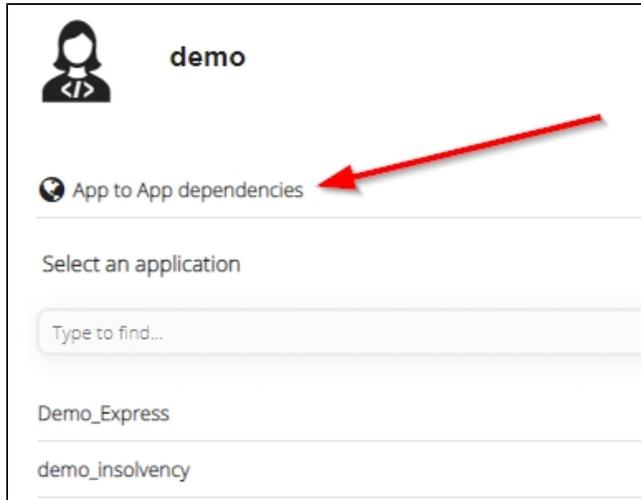| USER	The **USER** role should be granted to "standard" users/groups - i.e. those that do not require Admin Center access and limited resource p default set of resource permissions is as follows: *Click to enlarge*

Available resources

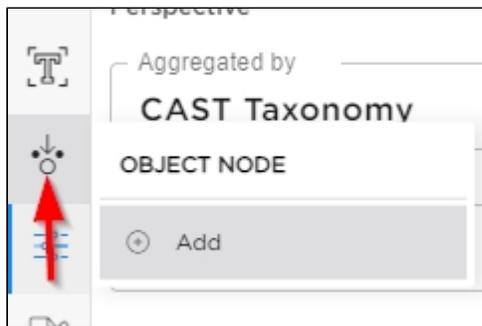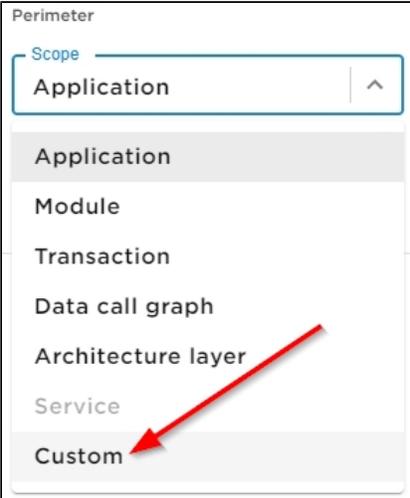| Admin Resources	Grants access to **admin level features** (available in the **Admin Center**) for the current tenant.

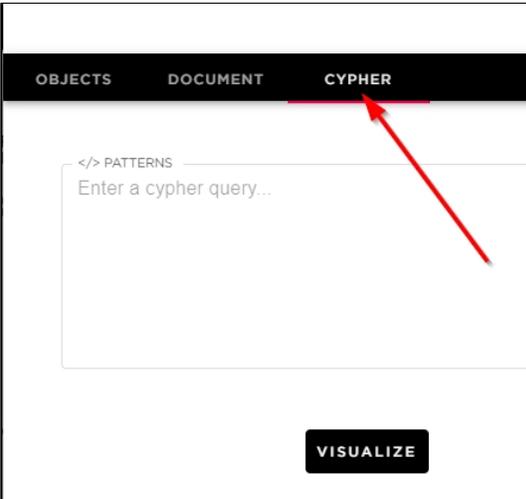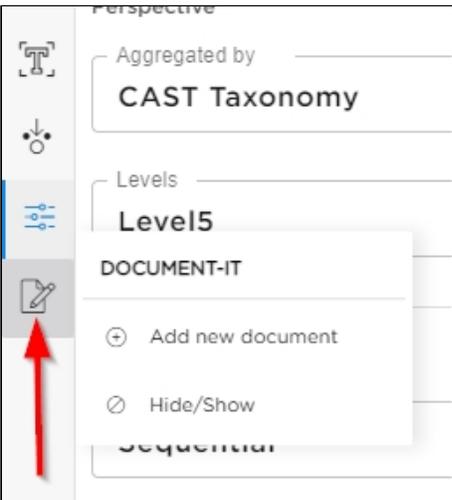|	
App to app dependencies	Grants access to the **User Guide - Application to Application dependencies scope** for the current tenant:
Custom Object Types	Grants access to the **custom node feature** for the current tenant:

Custom View	Grants access to the **User Guide - Custom scope** in the current tenant:
Cypher Search	Grants access to the **Cypher Search** feature for the current tenant:
Document-It	Grants access to the **Document-It** feature for the current tenant:

Services view	Grants access to the **User Guide - Service scope** for the current tenant: Perimeter Scope **Service** ⌄ Select Service **account-service** ⌄ ⓘ Note that this resource only has the ability to assign the CREATE permission.
Sourcecode viewer	Grants access to the **User Guide - Viewing source code** feature for the current tenant: ⓘ Note that this resource only has the ability to assign the CREATE permission.
Tags	Grants access to the **add tags** feature for the current tenant: Select ⦣ ⬭ TAG ⊕ Add CAST Taxonomy

Roles list

The Roles list displays the roles that are available for use and allows you to edit existing and create new roles:

Click to enlarge

	Roles ↑	Applications authority	Resources and permissions	
☐	Admin	All Applications ▾	Admin Resources App to App Dependencies Custom Object Types Custom View Cypher Search Document-It Services View Sourcecode Viewer Tags	✏
☐	Architect	Assign applications ▾	App to App Dependencies Custom Object Types Custom View Cypher Search Document-It Services View Sourcecode Viewer Tags	✏
☐	Super Admin	All Applications ▾	Admin Resources App to App Dependencies Custom Object Types Custom View Cypher Search Document-It Services View Sourcecode Viewer Tags	✏
☐	User	Assign applications ▾	App to App Dependencies Custom Object Types Custom View Cypher Search Document-It Services View Sourcecode Viewer Tags	✏

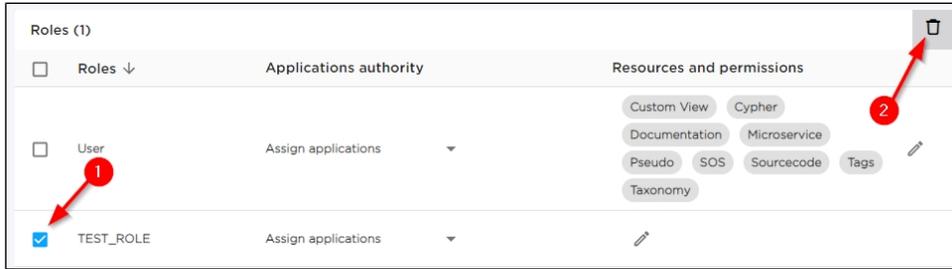| **Add role**	Add a new custom role:

New roles are created without any application data or resource permissions and must be manually configured before being assigned to

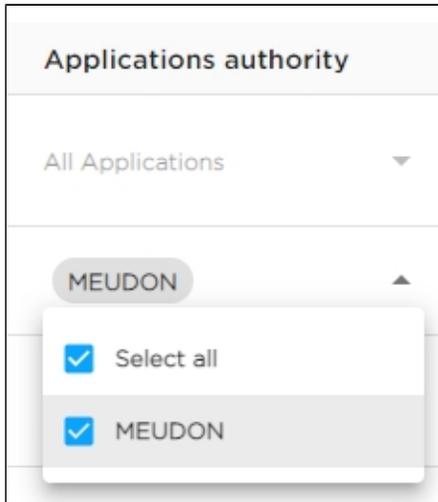|	
Selection box	Allows you to select the role and then delete the selected items:
Roles	Lists the names of the roles available in CAST Imaging
Applications authority	Lists any Applications that the user/group has been granted access to and allows Application data permissions to be changed:

Resources and permissions	Lists the resources that have been granted an access permission, and the ability to make changes:

Note that logic **checks** are performed when customizing resource permissions in this panel:

- On selecting a READ permission, the parent resource permission is automatically selected as well.
- If multiple permissions together with a READ permission are ticked for any resource, and then the READ permission is unticked, al and the parent resource permission will be automatically unticked.
- All the permissions for a resource will remain unchecked until a READ permission is ticked.

Assigning roles to users/groups

To assign a role or roles to your users or groups, use the **Admin Center - Users panel**:

Users (1)

☐	Users ↑	Roles
☑	cast	Admin Architect ▲
☐	test_user1	
☐	test_user2	

- ☐ Select all
- ☑ Admin
- ☑ Architect
- ☐ Super Admin
- ☐ User