Key Permission Components

Last Modified on 07/04/2019 10:38 am EDT

This section serves as a guide to the Resolver Core permissions model. It contains steps for providing users with access to appropriate information and links to relevant articles in the Core Admin Guide.

Core's permissions model uses a high level of detail to ensure that each user only sees the data they have been given access to. Due to the complexity of this model, it's important to understand the individual components of the permissions model and how those components work together.

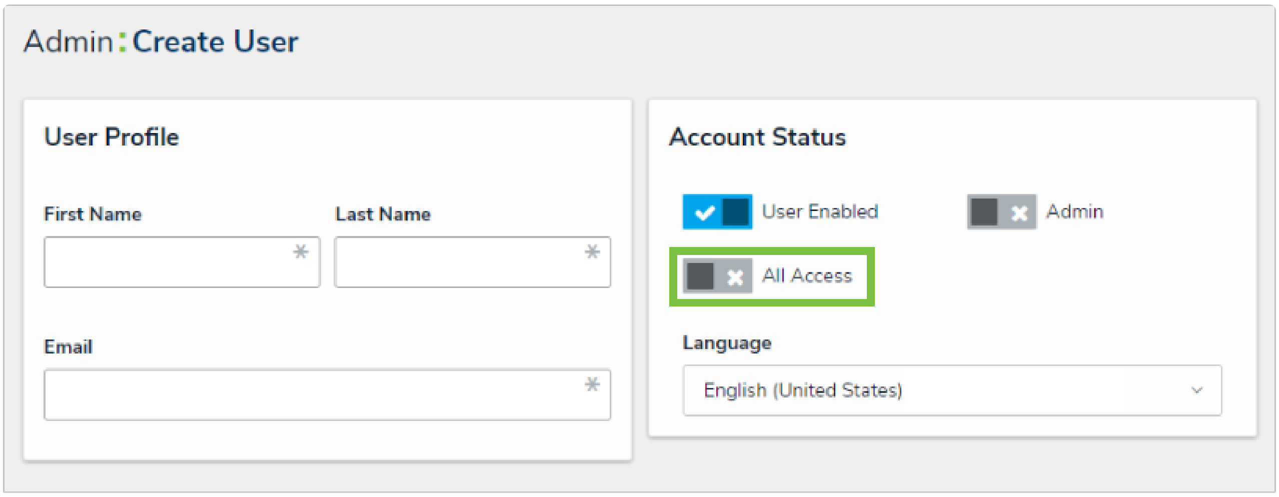
User Assignment: Users, User Groups & Roles

Permissions are configured by defining roles. Permissions can then be assigned within each role.

User groups are used to define multiple users to the same role. This allows roles to be granular, while reducing complexity. Users assigned to a user group will inherit the permissions for all roles assigned to the group. This is optional but recommended.

> Users may also be assigned directly to a role; however, this is generally not recommended, as adding users directly to roles will likely complicate your organization's permission model and any troubleshooting efforts should any permission-related issues arise.

User accounts also have an All Access setting, which is usually reserved for administrators only. If **All Access** is enabled, the user will have unrestricted access to all objects in the system without needing to assign roles or define permissions. This makes **All Access** useful for building new applications.



Admin: Create User

User Profile

First Name *

Last Name *

Email *

Account Status

✓ User Enabled

✗ Admin

✗ All Access

Language

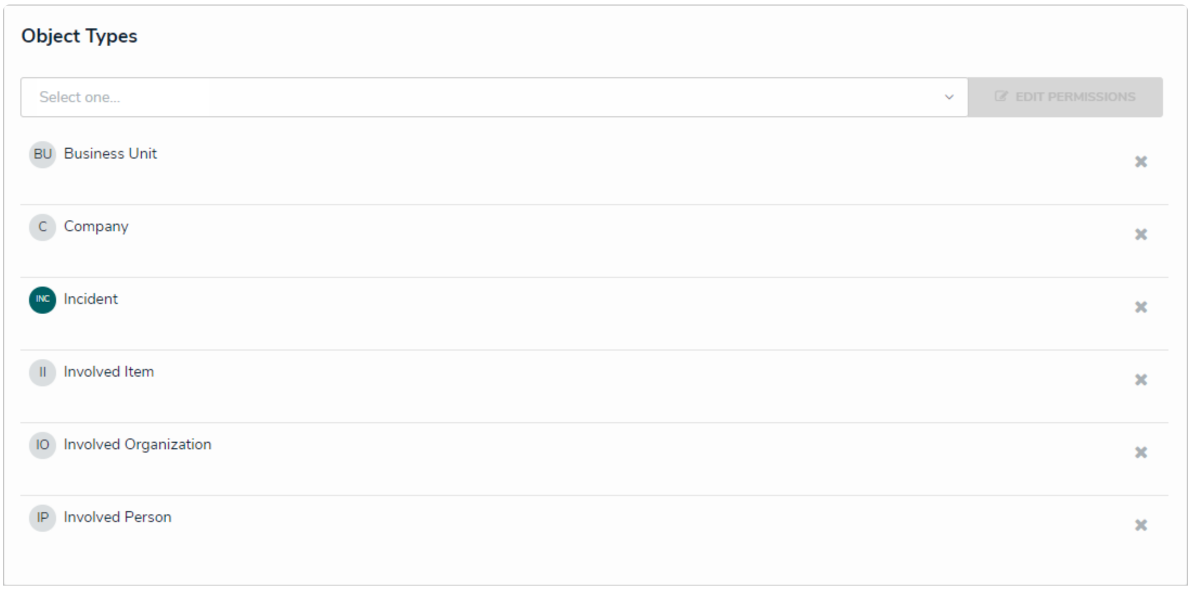
English (United States)

The Create User page, where the All Access feature can be found.

Role Configuration: Object Types, Workflows & Permissions

To configure a role:

1. Define the object types members of the role will have access to.



Object Types

Select one...

- BU Business Unit
- C Company
- INC Incident
- II Involved Item
- IO Involved Organization
- IP Involved Person

The Object Types section on the Edit Role screen.

2. Define the workflow permissions for each object type assigned to that role, including:

    a. Permissions: **Create**, **Read**, **Edit**, **Delete**, and **Manage**. (Selecting any of these permissions in the **All States** section will grant the role access to those permissions for all the workflow's states);

    b. Triggers (selecting **All Triggers** in **All States** will give the role the ability to click on all defined triggers);

    c. Objects assigned to the user's My Tasks list (**Assign**); and

    d. Forms the assigned user should see. This may still be overridden for specific:

    - Views
    - Report tables
    - Navigation forms
    - Relationship tables

3. If the role should have access to all objects from its assigned object types, enable Global Permissions when creating the role. Note that this setting cannot be changed once the role has been created.

4. If the users in the role should only have access to objects to which they have been explicitly assigned, some additional steps are required:

    a. Add the role to the object type and include it as a field on a standard form so users from the role can be assigned to an object. Once the user has been assigned to an object using that field, they will have access to that object in accordance with their role's definitions.

    b. **Optional:** Determine the main object type that the user needs access to (e.g. Risks for a Risk Owner, Business Unit for a Manager). On that object type, define the inferred permissions to specify the related object types that the user should inherit access to. By adding inferred permissions, the user is automatically granted access to related objects when they are assigned to the root object. For example, when a Risk Owner is assigned to a Risk, they will inherit permissions to any Controls linked to that Risk, and any Tests linked to that Control.

5. **Optional:** Disable the **Search**, **Quick Add**, and **Help** functions for the role.

Application/Activity Permissions

Roles can grant access to specific areas of Core by adding the role to an activity. This lets members of that role:

- Access the activity’s parent application in the **Nav Bar**.
- Access the activity through its tab at the top of the **Application** screen.
- Use the actions and views that have been added to the activity.

> Enabling **All Access** on a user’s account will **not** automatically grant access to all activities. The user must still be added to a role with access to the activity in order to access it.