Inferred Permissions Overview

Last Modified on 06/01/2021 3:20 pm MDT

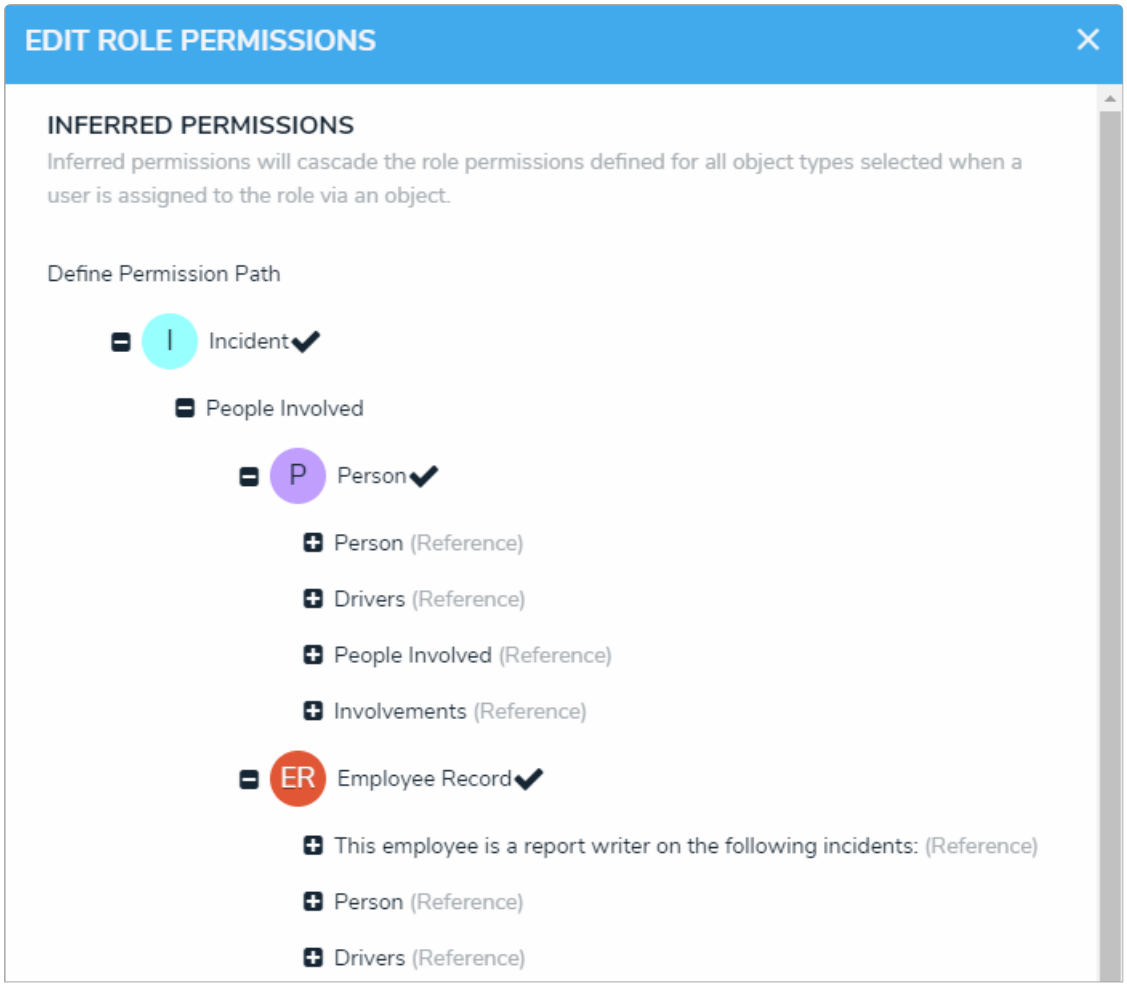
Inferred permissions allow you to give users with explicit permissions access to additional object types through relationships and references without directly granting permission through the role field on a configurable form. This ensures users within a particular role with explicit permissions are indirectly given the appropriate access to the information they need when interacting with related objects.

EXAMPLE

Hollie Peel is part of the Incident Editor role with explicit permissions. When working with existing incident objects, she may need to edit information about the people who were involved in an incident through the People Involved relationship, so she needs access to the Incident object type, as well as the Person and Employee Record object types. Therefore, the Incident, Person, and Employee Record object types are added to the Incident Editor role. After the role is configured, it's saved to the Incident object type as a component and is then configured to grant inferred permissions to the Person and Employee Record object types through the People Involved relationship. Once Hollie has been given access to an incident object (by being added to the Incident Editor role field on a form), she can edit the objects in the People Involved relationship without being granted direct access to People and Employee Record objects by another user.

Granting users inferred permissions is done using the following process:

1. Create a role.
2. Add the object types the user will have access to, including those accessed through inferred permissions, to the role.
3. Edit the workflow permissions for the object types. The rights granted here will determine the rights the user will have when accessing the object types through inferred permissions.
4. Add the role to the object type that has the relationships and references saved to it.
5. Edit the role on the object type to add inferred permissions.



Granting inferred permissions. The checkmarks next to the P (People) and ER (Employee Record) monograms confirm that users in that role have access to those object types through the I (Incident) object type.

After the above steps have been completed, a user with **Manage** rights must add a user who belongs to the selected role to an object through the role field on a configurable form. Once added, the user will have access to the object and any selected related objects based on the inferred and workflow permissions.

Users who are logged in at the time their role's permissions are configured will need to log out then log back in before the changes are applied.

Inferred permissions don't apply to objects that haven't transitioned out of the **Creation** state as the object has not yet been created and any users added to a role have not yet been saved.

Users with inferred permissions to an object will also receive email notifications related to that object, whether or not they are assigned to it.