Groups

Last Modified on 21/12/2020 8:46 pm ACDT

> This article is part of the systems administration guide. You will require administration access to view the pages mentioned in this article.

Groups ensure that the allocation of access rights is consistent across similar groups of staff. Changes made to a security group, affect all users who have that group assigned.

Groups serve two main purposes:

- Define what a group of users can do; and,
- Define what locations a group of users can see (i.e. patients at that location).

Create a New Security Group

1. Click **Groups** link.
2. Click **Create New**.
3. Give the Group a **Name** and **Description**.
4. Click **Create Group** – the new group is saved and the Allowed Actions screen displays.
5. Tick any **Allowed Actions** that member of the group should be able to perform.
6. Click **Update Group**.

Editing Allowed Actions

To change the Allowed Actions that a group can perform:

1. From the Groups page, click the **Edit** link.
2. Tick or un-tick each **Allowed Action** for the group - these are self explanatory but contact us if you are unclear.
3. Repeat until the satisfied and click **Update Group**.

Allocate Locations

In order for a user to access patients at a location, they need to have access to said location. This is normally done by allocating a location to a group that they are a member of.

1. For the group click **Show**.
2. At the Location Allocation grid, click **Create New**.
3. Select a location from the list and edit the start date if required.
4. **End Date** can be used if a groups access is restricted to a period of time (e.g. a Contractor or Locum).
5. Click **Create**.
6. Multiple locations can be added to a Group.

Location Allocations that no longer apply to the group should have the end date set in the 'Valid To" field (via the Edit link).

Setting up Groups for a Multi-site organisation

See <u>Scenarios > Groups - Location based setup</u> for a practical example of setting up groups for multi-site organisations.

Delete a Security Group

If a group is created in error, and no users are members, then it can be deleted:

1. Click the **Groups** link.
2. Click the **Destroy** link of the group you wish to delete.
3. Click **OK** to the confirmation message that appears.

You can only delete a group that is not is use.

v6.62 Feature: Create Datasets

This specification adds the ability to create datasets between staff members groups and roles.

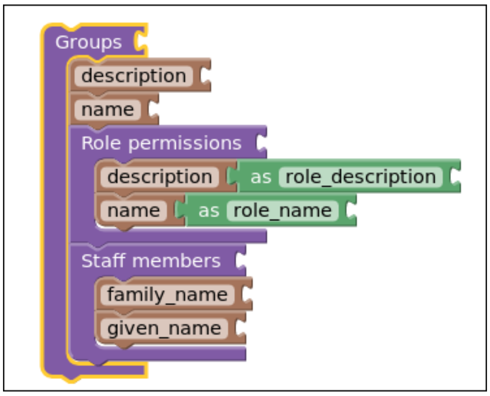
There is a need to expose the following to datasets:

- Groups – with the following fields
  - name
  - description
- Roles – with the following fields
  - name
  - description

Applicable joins:

- StaffMember -> Groups
- Groups => StaffMember
- Groups -> Roles
- Roles <- Groups

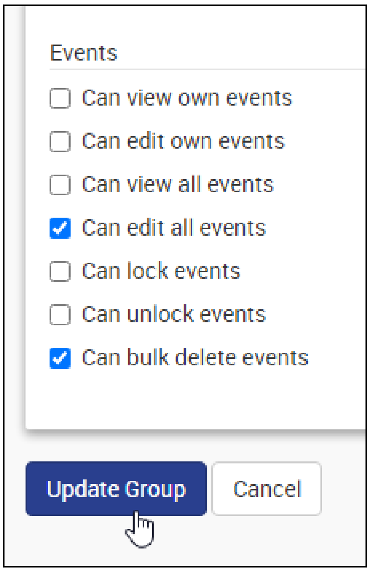
In Visual Query Builder:



v6.69 Feature: Bulk Delete Events

A new permission, **Can Bulk Delete Events**, has been added to the list of group privileges. Enabling this permission—in conjunction with the **Can Edit All Events** permission—enables a user to delete multiple events using a bulk deletion tool.

For more information, please see Events.



v6.70 Feature: Allowed Actions Category → Cases

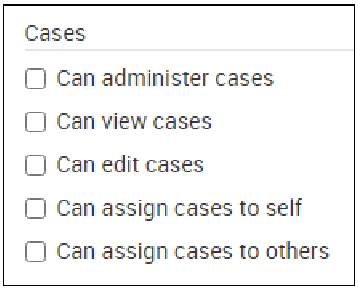
Due to several enhancements to the management of cases in v.6.70, a new allowed actions category has been created called Cases.

This category includes the following two new permissions:

- "Can assign cases to self" (case_assign_self)
- "Can assign cases to others" (case_assign_others)

...and also includes existing case role permissions

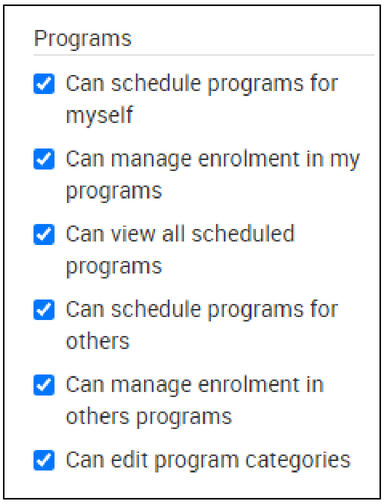
- "Can view cases" (case_viewer)
- "Can edit cases" (case_editor)
- "Can administer cases" (case_admin)



v6.70 Feature: Allowed Actions Category → Programs

Due to the introduction of the new Programs functionality in CareRight, there is now a new allowed actions category has been created called Programs.

The permissions listed below are all new.



v6.71 Feature: Allowed Actions Category → Patient Accounts

In this version we introduced the following new permissions:

Can edit Provider / Service Location after Invoice created

This permission relates to whether or not users have the ability to edit a medical provider and/or a service location directly within an invoice. For some companies, this capability is highly useful while, for others, it creates operational challenges. Therefore, in this version of CareRight, we now offer these capabilities as a role-based permission that can be toggled on or off depending on business/operational requirements.

Separation of Account Transaction Permissions

Prior to version 6.71, all advanced billing manipulation was controlled by a single billing permission (account_unrestricted_transactions). From v6.71 onwards, permissions have been split off to provide more granular control over specific permissions that can be assigned to users.

These new permissions are:

- **Can edit account transactions (restricted)**
  - This is used to backdate transaction dates when manually applying batch payments and to change the statement date on invoice/receipts during creation.
- **Can alter general ledger codes older than the current date**

- **Can overpay invoices and reallocate combined payments**
    - User can overpay invoices that are already paid when allocating receipts manually and user can reallocate combined payments.
- **Can alter guarantor on used patient accounts**
    - User can alter a patient account guarantor, location or provider after transactions have already been recorded.
- **Can reverse receipts and invoices older than the current date**
    - Users can reverse statements and invoices older than the current date and can refund receipts older than the current date.