Roles and Permissions

Default Roles

Every project begins with five default roles with varying degrees of access to CommCareHQ. This section briefly summarizes these roles. For a detailed description on what each role can and cannot do, please look to the permission descriptions below.

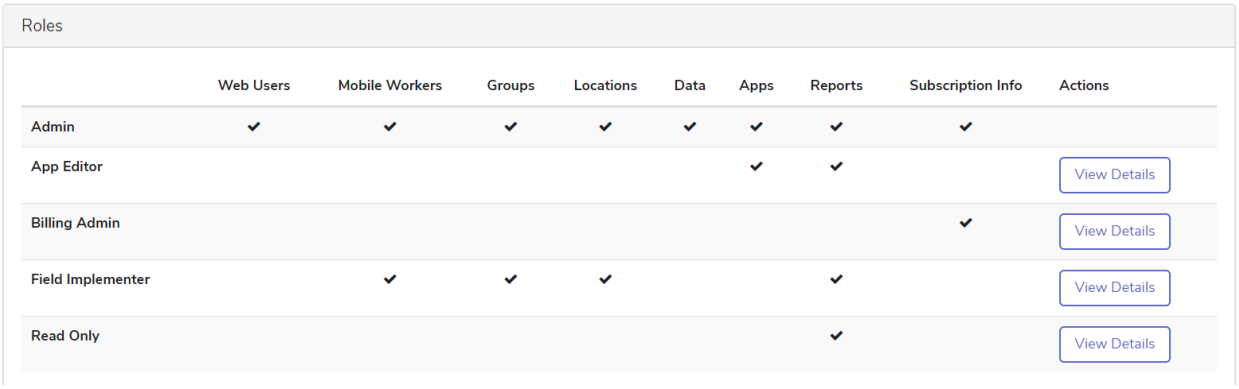
Admin: Admins have complete access to your project space on CommCareHQ. They can add, edit and delete data, along with creating and editing applications.

App Editor: App editors have partially restricted access to CommCareHQ. They cannot access users, groups or locations but can access App Builder and Form Builder. Additionally, they can access reports and exports.

Billing Admin: Billing admins can largely only access subscription information.

Field Implementer: Field implementers can edit data that relates to mobile workers, including locations and groups

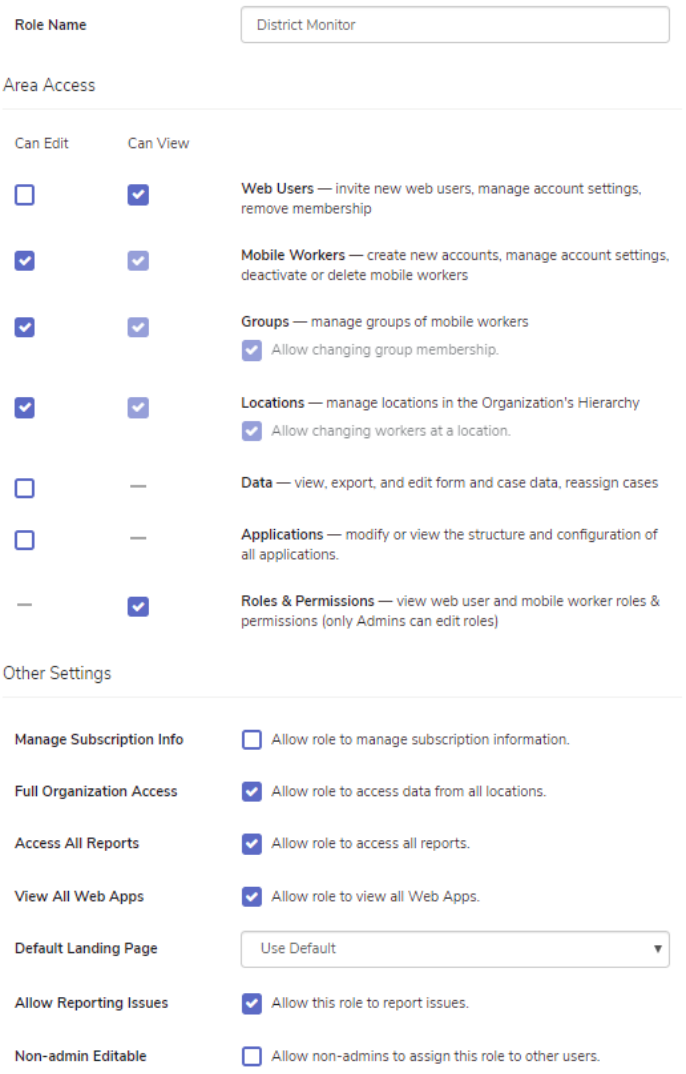
Read Only: Users with the Read Only role will be able to access reports and exports, but little else.



Configure User Roles

> This feature (Advanced Role-Based Access to CommCareHQ) will only be available to CommCare users with a Standard Plan or higher. The default roles, however, will be available to everyone. For more details, see the CommCare Software Plan page.

You can create custom project roles and give these roles the desired permissions for accessing parts of your project space. To do this, select the Users tab, then Roles and Permissions. Once on this page, you can choose to add a new role, or to edit any existing role, other than Admin. Either action will trigger the modal seen below:



Most Area Access permissions come with multiple layers of access:

Can Edit: With Edit access enabled for a permission, users can create, edit and delete corresponding data. For example, if a role had Can Edit enabled for mobile workers, users assigned to that role could create, edit and delete mobile workers.

Can View: If Can Edit is disabled, the Can View checkbox becomes editable. Enabling Can View allows users with this permission to see all corresponding data, but not edit it. For example, if a role had only Can View enabled for Web Users, they could see all Web Users but not invite new users nor edit or remove existing users.

No Access: (both Edit and View deselected): If both Can Edit and Can View are disabled for a permission, users will have no access to the corresponding data. This setup removes references to that data from the top and sidebar navigations in CommCareHQ for all associated users. For example, if a role had Can Edit and Can View disabled for Groups, a user with that role would see no links to Groups under the Users tab. If that user navigated directly to groups, say by typing in the URL line, they would receive a 403 error.

Descriptions of these roles can be found here:

Area Access Permissions

Web Users	Invite new web users, manage account settings, remove membership. This permission will be hidden if Full Organization Access is disabled.
Mobile Workers	Create new accounts, manage account settings, deactivate or delete mobile workers

Groups	Manage groups of mobile workers This permission will be hidden if Full Organization Access is disabled.
Groups (Sub-permission)	Allow changing group membership This permission allows you to assign mobile workers to a group. This is typically controlled by the "Edit Mobile Workers" permission, but this option may be useful if you need users who can edit group membership, but not otherwise edit mobile worker data.
Locations	Manage locations in the Organization's Hierarchy
Locations (Sub-permission)	Allow changing workers at a location This permission allows you to assign mobile workers to a location. This is typically controlled by the "Edit Mobile Workers" permission, but this option may be useful if you need users who can edit location membership, but not otherwise edit mobile worker data.
Data	View, export, and edit form and case data, reassign cases
Applications	Modify or view the structure and configuration of all applications. This permission will be hidden if Full Organization Access is disabled.
Roles & Permissions	View web user and mobile worker roles & permissions (only Admins can edit roles) This permission is 'View Only' for all roles except Admins. View access can be deselected to prevent users from viewing Roles & Permissions entirely. This permission will be hidden if Full organization Access is disabled.

Other Settings Permissions

Manage Subscription Info	Allow role to manage subscription information. Subscription info can be found under your project settings. This permission will be hidden if Full organization Access is disabled.
Full Organization Access	Allow role to access data from all locations. If disabled, your users must be assigned locations in order to access CommCareHQ. Disabling this permission renders obsolete Web Users, Groups, Applications, Roles & Permissions and the Manage Subscription Info permissions and hides them from view. For further information, please see the Full Organization Access sub-section.
Access All Reports	Allow role to access all reports. If this permission is disabled, you have the option to grant access to individual reports.
Default Landing Page	Upon login, the permission decides where the user begins; on the Dashboard, Web Apps or Reports. If Use Default is selected, mobile workers will be directed to Web Apps and Web Users will go to the dashboard.
Allow Reporting Issues	Allow this role to report issues. This permission is enabled by default.
Non-Admin Editable	Allow non-admins to assign this role to other users. Users can assign roles on the Web Users page

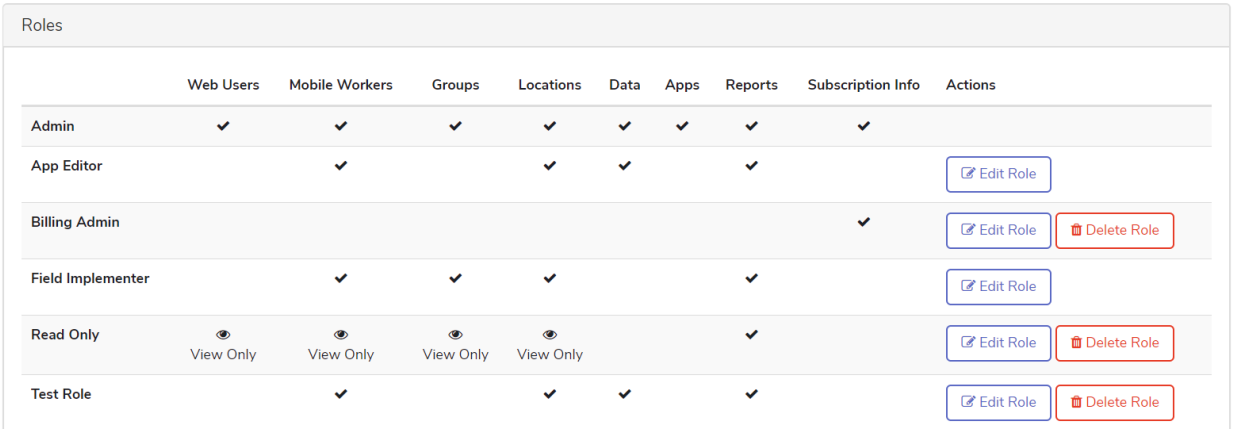
Full Organization Access

The Full Organization Access permission is very powerful and if disabled, can severely limit what a user can see on CommCareHQ.We highly recommend that you test the implications of disabling this permission before rolling it out to your project.

Creating a locations-restricted user by disabling Full Organization Access may be helpful to your workflow if you have a role similar to a 'District Manager,' for example. A District Manager may need to access reports and exports, but may only need data restricted to specific locations. This role would not be able to edit apps, but could view all data in reports/exports from their assigned location and those locations under it.

Deleting Roles

The Delete Role button is only accessible when no users are assigned to a role. In the below screenshot, users are assigned to the Field Implementer role and therefore, we cannot delete it.


Roles
Web Users
Mobile Workers
Groups
Locations
Data
Apps
Reports
Subscription Info
Actions
Admin
App Editor
Edit Role
Billing Admin
Edit Role
Delete Role
Field Implementer
Edit Role
Read Only
View Only
View Only
View Only
View Only
Edit Role
Delete Role
Test Role
Edit Role
Delete Role