# Roles & Permissions Administration

Download the PDF of this article.

In this Article

Related Articles

## Overview

Each user must be assigned to a role.

Every role has a different set of permissions. You can assign a user to the best-fitting role, or create a new role.

You may **create roles to give more restrictive permissions** to a group of users, e.g., you can prevent those users from editing the branding of their forms, or enforce a form publishing approval process. If a user attempts to use an option that they don't have access to, a message will be displayed to notify them that the **option is not available with their current role**.

You may customize this error message to reflect your organization policies or practices. To do so, go to **Admin Dashboard | Settings | Permission Messages** and edit the Permission Related Messages.

## Requirements

**Enterprise** **Compliance Cloud**

For information on upgrading, please contact our Sales Department at sales@formassembly.com.

## Default Roles

There are two roles by default: Administrator and Author.

An **Author** can create their own forms and collect data. They cannot access the Administration area and therefore cannot create users, access other users' data, or change the application configuration options.

An **Administrator** can see the Admin tab and access the Administration area of the application. They can create users, impersonate existing users, view existing forms, browse collected responses, delete data, and configure the application.

## Create a New Role

1. Browse to: **Admin Dashboard | Settings | User Roles**
    - The **User Roles** tab contains the list of roles available in the application.
2. Click **Add Role** at the bottom of your existing list of roles.
3. Choose a name for the new role.
4. Set the permissions by clicking the appropriate boxes.
5. Click **Apply** below the options.

## Modify an Existing Role

1. Browse to: **Admin | Settings | User Roles**
2. Click the title of the role you would like to edit.
3. Modify the permissions by clicking the appropriate boxes.
4. Click **Apply** below the options.

# Sensitive Data Management on Compliance Cloud

For enhanced data governance and security, Compliance Cloud administrators can manage who can collect or view and edit responses containing sensitive data. Learn more about sensitive data.

### Professional, Premier, and Enterprise Cloud accounts

- PII and General Sensitive Data are always enabled and cannot be disabled for any user role.

### Compliance Cloud accounts

Each sensitive data type permission can be enabled or disabled for a user role:

**PII**

- Create and edit forms with PII
- View and edit responses with PII

**PHI**

- Create and edit forms with PHI
- View and edit responses with PHI

**General Sensitive Data**

- Create and edit forms with General Sensitive Data
- View and edit responses with General Sensitive Data

---