Team Management Overview

WorkStep enables administrators the ability to manage team members' access to your organization's account. Administrators can create and manage team members and their access from the **Team** area. This is a fundamental security feature providing only administrators full control over who accesses the account, and what authorizations they are enabled, from a granular level.

Access and authorization permissions

Users can only access the system once they are configured as part of the **Team** by an administrator.

Access to different features is then controlled by:

- Module (separately for the Hire and Retain modules), role and facility
- Authorization to perform actions: view-only, edit or admin

The following table describes the kind of authorization enabled for each of the different levels.

Permission level	***Access breadth***
Retain module	
Admin	Enable and configure Check-Ins. View the **Team** page and invite new team members.
Editor	Reply to Alerts and Comments.
View-Only	View Check-In responses for the facilities assigned to them.
Hire module	
Admin	View the **Team** page and invite new team members. Create new job roles.
Editor	Take action on roles.
View-Only	View all content for the role (can't take action on the role).

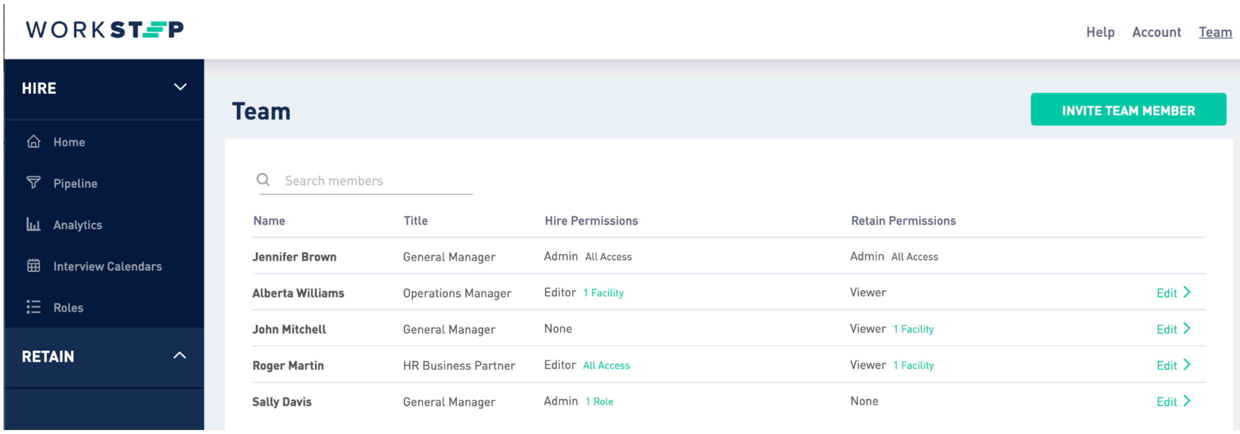
The ability to configure access on this granular level means that any user can only access the areas configured for them and can only view, edit or manage in those areas based on the authorization level configured for them.

For example, a user assigned an admin role for all facilities and roles in the **Retain** module and view-only for **Hire** can see all users in the **Team** area, can manage the users in the **Retain** module, and can only view details in the **Hire** module.

All administrators (regardless of their configured limitations) can access the **Team** area and from its main page, they can view a complete list of all users in the organization. This provides better visibility and transparency into company-wide access and use of **WorkStep**.

Team area overview

Click **Team** from the top right of any screen in **WorkStep** to manage users. The main page of the **Team** area loads, automatically sorted alphabetically by user name:



Super admins can see and manage user access for both **Hire** and **Retain** on the same page. Admins for one or the other **Hire** and **Retain** module can see the associated column for that module: **Hire** admins see the **Hire** column and **Retain** admins see the **Retain** column.

To change the sort, click on the relevant column name.

Invite team members

Administrators grant access to facility and role level data based on what that specific admin user has access to. For example, if User X has “all access” then they can grant “all access” to other users. If they only have access to the “San Francisco” facility, then they can only grant access to the “San Francisco” facility.

To invite a new user:

1. Click **Invite Team Member** from the top right of the **Team** area to invite new users.
   The **Invite Team Member** screen loads.
2. Configure the user’s access and click **Save**.
   The invite is sent to the user based on the email you entered. When they access the system, they will be able to perform actions and view information based on the way you configured their role.

Read more [here](#) for information about configuring roles.

Edit Team Member

Administrators grant access to facility and role level data based on what that specific admin user has access to. For example, if User X has “all access” then they can grant “all access” to other users. If they only have access to the “San Francisco” facility, then they can only grant access to the “San Francisco” facility.

To edit permissions:

1. Find the user whose permissions you want to update.
2. From the row for that user, click **Edit.**
3. Configure the user’s access and click **Save** to update the user’s permissions.

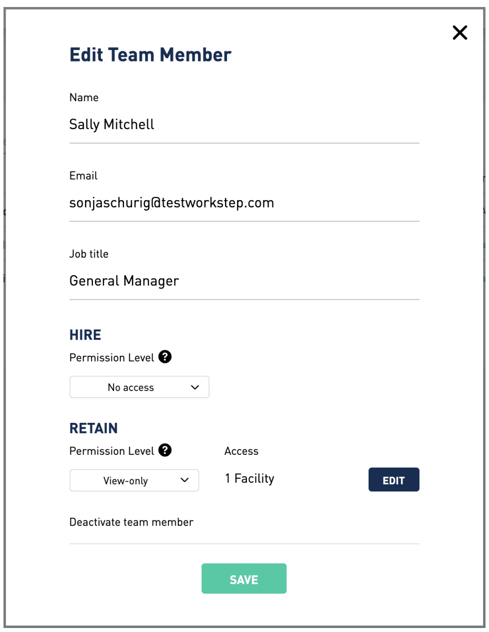
Read more here for information about configuring roles.

Configure permissions

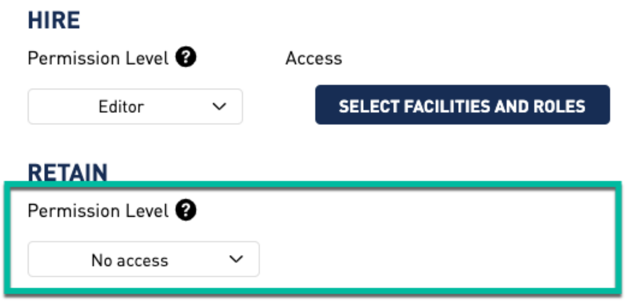
Every time you invite a new user or edit an existing user, you access the same fields, enabling you to update their details and their permissions.

To configure permissions and details:

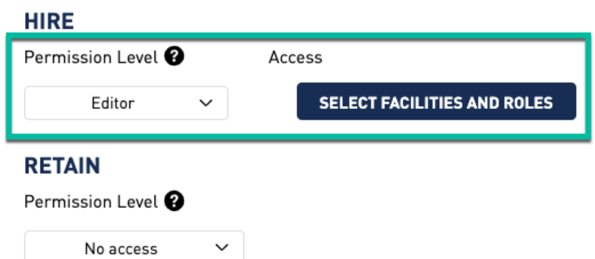
1. Access the screen by clicking Invite Team Member or finding an existing user and clicking Edit. A screen loads similar to the following:



2. Enter relevant details for the name, email and job title of the user.
3. To configure permissions for each of the **Hire** and **Retain** modules, go to their area towards the bottom of the screen and select the relevant permission level from each of their dropdown lists. If no permissions are configured at all yet, only **No access** appears in the **Permission Level**:



If a permission level is selected but the access scope has not been, then the level appears in the **Permission Level** and the **Select Facilities and Roles** button also appears next to it:

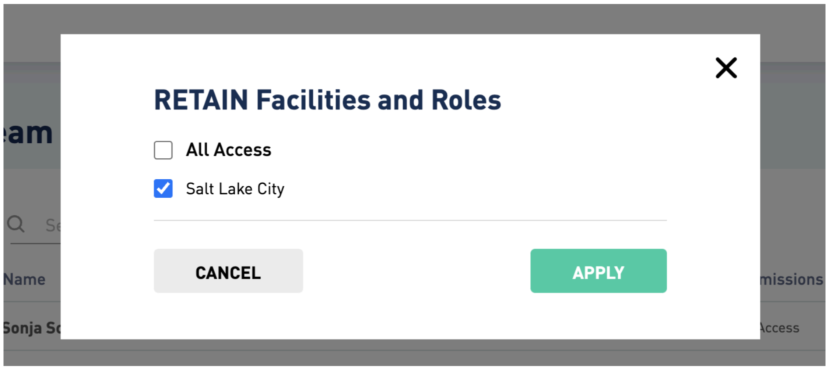


Note: you can't save your changes until you add the access scope.

If a permission level is selected and the scope is also already configured, then the level appears in the **Permission Level**, the **Access** scope appears and the **Edit** button also appears:

4. To configure or change the permission level, select the relevant option from the dropdown list. Read more here for information about different permissions levels.
   The main configuration window pops up.
5. To configure or change the access scope, ensure you've already selected a permission level other than **No access** and then click the button - either **Select Facilities and Roles** or **Edit**.
   A screen similar to the following pops up, listing all available facilities and roles for the specific

module:



6. Select the facilities and roles to which this user can have the selected permission level access and then click **Apply**.
   This pop-up closes and you can continue working from the main configuration window.
7. When finished updating the user configuration and details, click **Save**.
   The user is updated, tmain **Team** area updates based on your changes, and the configuration window closes.

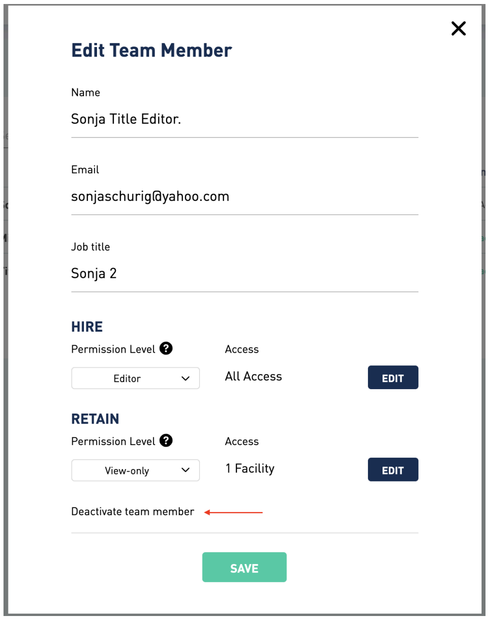
Deactivate Team Member

You can deactivate team members whenever you need to - this can be useful when an employee leaves your organization or even just changes roles. When you deactivate a user, they are completely removed from the system and they can no longer access it at all. Only admins with “all access” can deactivate another user.

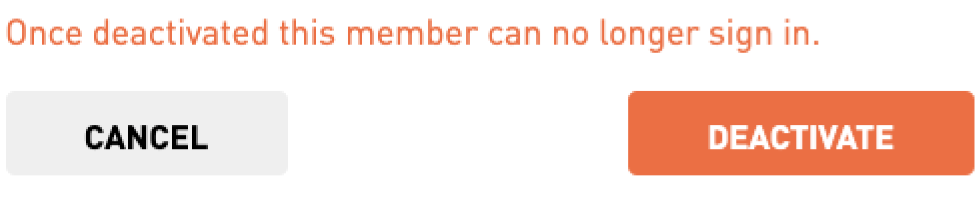
To deactivate a user:

1. Find the user whom you want to remove.
2. From the row for that user, click **Edit.**

3. The Edit Team Member window pops up:



4. Click the **Deactivate team member** link from the bottom of the window.
   A confirmation reminder and a **Deactivate** button appear in the window:



5. To remove the user, click **Deactivate**.
   The user is removed from the system, the window closes and the user list in the main Team area reloads.
   Note: to exit without removing the user, click **Cancel**.