

Onboarding - User Groups and Permissions

Last Modified on 10/02/2026 3:04 pm CDT

Understanding User Groups and Permissions

Every user's access comes from the user groups they belong to. This article explains how groups, permissions, and access rules combine to control who can see and do what.

Roles are not assigned to individual users. Instead, you add each user to one or more user groups, and every group provides two things:

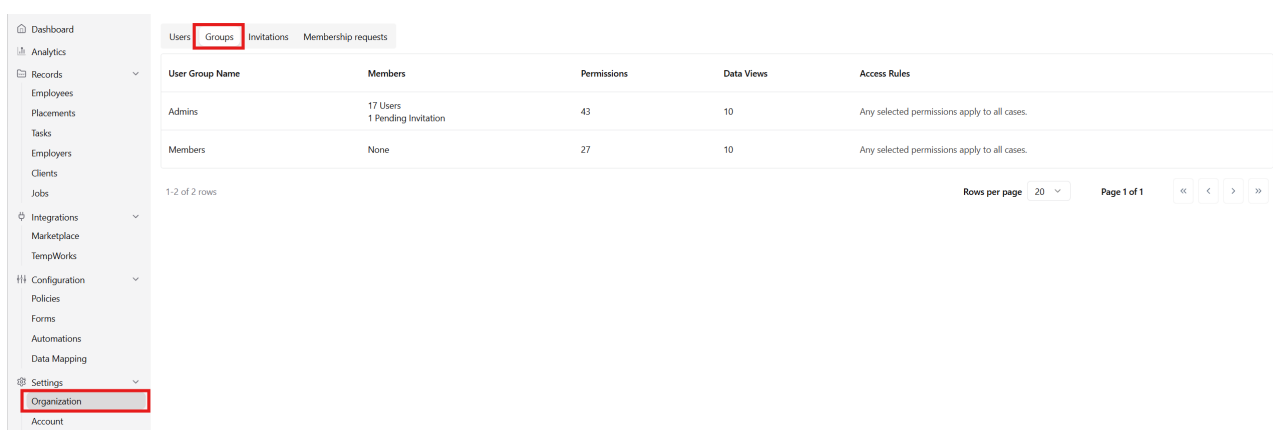
- **Access Rules:** Optional conditions that narrow which records permissions apply to.
- **Permissions:** The actions that members of the group can take, per record type. View, create, edit, and delete for Employees, Jobs, Tasks, Placements, Employers, and Clients, plus admin-level areas like Forms and Policies.

Default User Groups

There are two default user groups that are accessible within the Onboarding Portal:

- **Admins:** Contains every permission including the ability to manage Forms, Policies, User Groups, Custom Views, and API Tokens.
- **Members:** Contains permissions that allow the ability to view, create, edit, and delete record types including Employees, Jobs, Tasks, Placements, Employers, and Clients.

User Groups can be accessed via Settings > Organization > User Management > Groups:



User Group Name	Members	Permissions	Data Views	Access Rules
Admins	17 Users 1 Pending Invitation	43	10	Any selected permissions apply to all cases.
Members	None	27	10	Any selected permissions apply to all cases.

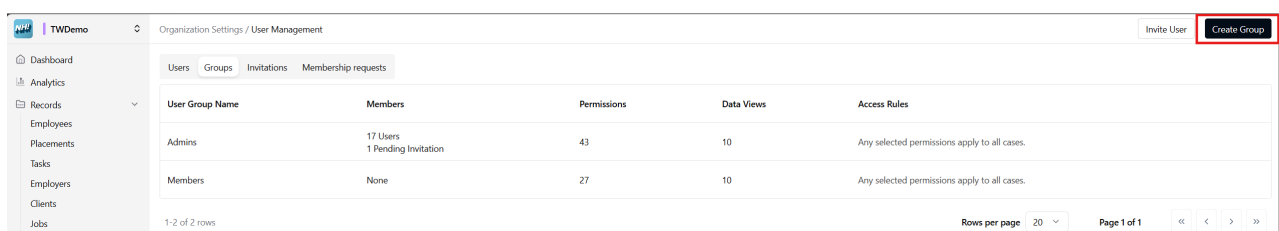
1-2 of 2 rows

Rows per page: 20 Page 1 of 1

Note The default user groups do not start with access rules, meaning that users will be able to see all records for the records they're granted. You can edit both default groups, or create your own with separate access rules.

Creating a User Group

Begin by selecting the "Create Group" option at the top right:



Within the "Create a new user group" window, enter a name for the User Group and then select the appropriate "Access Rules" and "Permissions".

Note For example, a company staffs light-industrial jobs across two regions and wants Regional Coordinators to manage candidates without the ability to delete records.

The Administrator creates a User Group titled "Central Coordinators" with the permissions "View Employees", "Edit Employees", "View Tasks", and "Edit Tasks", and one Access Rule of "employee.custom_attributes.region is Central". Regional Coordinators in that User Group can update candidate records and work onboarding tasks for the Central region. They are unable to delete records, see the other region's candidates, nor modify Forms or Policies.

In the event those same Regional Coordinators are needing administrative access, there is no need for the User Group to be modified. Instead, they will be added to the default "Admins" User Group, granting them all the necessary permissions.

Access rules

Access rules are conditions evaluated against each record.

For example, an access rule of "employee.custom_attributes.tempworks_branch_name is Minneapolis" means that a user group with that access rule and the "View Employees" permission will only see candidates whose are within the "Minneapolis" branch:

Access Rules ?

OR ▼

Any of the following must be true

Tempworks Branch ... ⌵

is ⌵

Minneapolis

Aa

+ Add condition

+ Add group ▼

✧ Thinking...

Permissions

⚠ Granting permissions without any access rule condition for the entity will grant access to all records of the entity type.

- ☒ **View Employees**
Can view employee information and details
- ☐ **Edit Employees**
Can edit employee information and details

Note Rules can only reference properties marked as a "Permission Scope". If a property you expect isn't available in the rule builder, you will need to enable the "Permission Scope" for that custom attribute.

Navigate to Settings > Organization > Custom Attributes:

Dashboard

Analytics

Records ▼

Employees

Placements

Tasks

Employers

Clients

Jobs

Integrations ▼

Marketplace

TempWorks

Configuration ▼

Policies

Forms

Automations

Data Mapping

Settings ▼

Organization

Account

Management

📅 **Edit Organization**
Update organization details

👤 **Custom Attributes**
Manage custom attributes

👥 **User Management**
Manage users, groups, and invitations

🏷️ **Tags**
Manage form tags

Search for the custom attribute and once found and select "Edit":

WPS | TWDemo

Organization Settings / Custom Attributes / employee.custom_attributes.tempworks_branch_n...

Deprecate

Edit

Delete

Dashboard

Analytics

Records

Employees

Placements

Tasks

Employers

Clients

Jobs

Integrations

Marketplace

TempWorks

Configuration

employee.custom_attributes.tempworks_branch_name

Entity Type

employee

Name

tempworks_branch_name

Path

employee.custom_attributes.tempworks_branch_name

Scalar Type

string

Label

Tempworks Branch Name

Description

Status

Active

Searchable

Yes

Sensitive Info

No

Permission Scope

No

Select the checkbox to enable the Permission Scope, and select "Update Custom Attribute":

employee.custom_attributes.tempworks_branch_name

Entity

Employee

Name

tempworks_branch_name

Name determines how this property can be set and returned from the entity API. For example, when working with employee custom attributes, add the prefix `employee.custom\_attributes.` to the property name in the field path. The same prefix is needed when setting and reading submissions for fields under this property via the Task API. When working with employer custom attributes, use the prefix `employer.custom\_attributes.` instead.

Scalar Type

String

Validation Regex

e.g. `^\d{3}-\d{2}-\d{4}$`

Optional regular expression to validate submitted values. Leave blank to allow any value.

Label *

Tempworks Branch Name

Label will be displayed as field label in core entity new/edit form next to the input that collects value for this custom attribute. Choose a value that helps customers understand what value they should enter for this custom attribute.

Description

Description will be displayed as hint in core entity new/edit form next to the input that collects value for this custom attribute. Use this field to help customers understand the appropriate value they should enter for this custom attribute.

☒ Searchable ?

☐ Sensitive Information ?

☒ Permission Scope ?

Cancel

Update Custom Attribute

Once updated, the rule can be enabled within the creation of the user group.

Note Granting a permission without any access rules for that entity will result in users having access to **all** records of that type. If a group is meant to see only specific records, ensure that rules are created for those entities.

Permissions

Each permission pairs a record type with an action. Examples include:

- View Employees
- Edit Employees
- Create Jobs
- Delete Tasks
- Etc.

Note Edit, create, and delete permissions each depend on the matching view permission. For example, you are unable to grant the "Edit Employees" permission to a group that doesn't also have the "View Employees" permission.

Permissions

 Granting permissions without any access rule condition for the entity will grant access to all records of the entity type.

☒ **View Employees**
Can view employee information and details

☒ **Edit Employees**
Can edit employee information and details

☒ **Create Employees**
Can create new employees

☐ **Delete Employees**
Can delete employees from the system

☒ **View Jobs**
Can view job information and details

☒ **Edit Jobs**
Can edit job information and details

The following permissions are able to be selected when creating/editing a user group:

- View/Edit/Create/Delete
 - Employees
 - Jobs
 - Placements
 - Tasks
 - Employers
 - Clients
 - Custom Views
 - Policies
 - Forms
 - User Groups
 - API Tokens

Once you have selected the permissions intended for the user group, you can now add or invite users:

Users

+ Add Users

Email

joshua.kramer@tempworks.com



Invitees

+ Add Invitations

Email

No results.

Once the users have been added, select "Create User Group" to complete the setup:

Users

+ Add Users

Email

joshua.kramer@tempworks.com



Invitees

+ Add Invitations

Email

No results.

Cancel

Create User Group

With the User Group created, should you have the necessary permissions, you can then either "Edit" or "Delete" the User Group via their respective options within the "User Group" page:

Members

Basic Information

ID	ug_01k-jr4s1ffazkrm1bu1bhs8d2
Permissions	employee:read employee:edit employee:create employee:delete job:read job:edit job:create job:delete
	task:read task:edit task:create task:delete placement:read placement:create placement:delete employee:read
	employer:edit employer:create employer:delete client:read client:edit client:create client:delete form:read
	form:edit form:create form:delete

Related Articles