
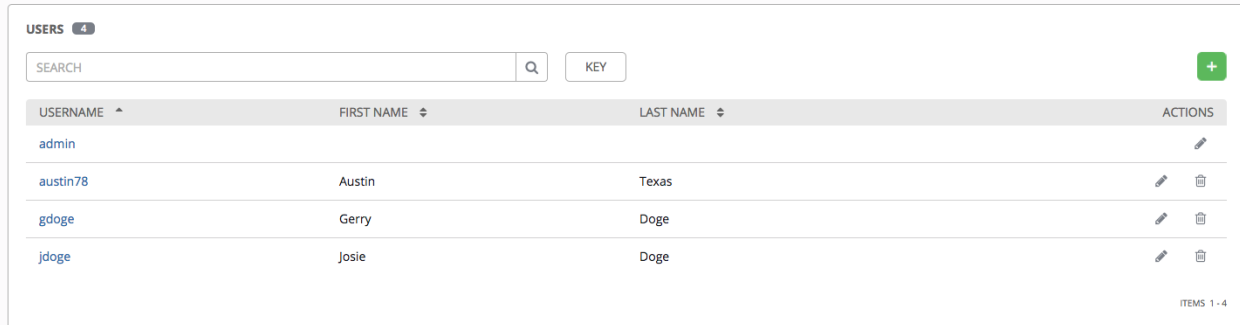









## 8. Users

A [User](#) is someone who has access to Tower with associated permissions and credentials.

Access the Users page by clicking the Users () icon from the left navigation bar. The Users page allows you to manage all Tower users. The User list may be sorted and searched by **Username**, **First Name**, or **Last Name** and click the headers to toggle your sorting preference.




USERNAME ^	FIRST NAME ^	LAST NAME ^	ACTIONS
admin			
austin78	Austin	Texas	 
gdoge	Gerry	Doge	 
jdoge	Josie	Doge	 

ITEMS 1 - 4

### 8.1. Create a User

To create a new user:

1. Click the  button, which opens the Create User dialog.
2. Enter the appropriate details into the following required fields:
  - First Name
  - Last Name
  - Organization (Choose from an existing organization–this is the default organization if you are using a Self-Supported level license.)
  - Email
  - Username
  - Password
  - Confirmation Password
  - User Type

#### Note

When modifying your own password, log out and log back in again in order for it to take effect.

Three types of Tower Users can be assigned:

- **Normal User:** Normal Users have read and write access limited to the resources (such as inventory, projects, and job templates) for which that user has been granted the appropriate roles and privileges.
- **System Auditor:** Auditors implicitly inherit the read-only capability for all objects within the Tower environment.
- **System Administrator:** A Tower System Administrator (also known as Superuser) has full system administration privileges for Tower – with full read and write privileges over the entire Tower installation. A System Administrator is typically responsible for managing all aspects of Tower and delegating responsibilities for day-to-day work to various Users. Assign with caution!

USERS / CREATE USER

NEW USER

DETAILS

ORGANIZATIONS

TEAMS

PERMISSIONS

\* FIRST NAME

\* LAST NAME

\* ORGANIZATION

Q

\* EMAIL

\* USERNAME

\* PASSWORD

SHOW

\* CONFIRM PASSWORD

SHOW

USER TYPE

Normal User

Normal User

System Auditor

System Administrator

CANCEL

SAVE

## Note

The initial user (usually “admin”) created by the Tower installation process is a Superuser. One Superuser must always exist. To delete the “admin” user account, you must first create another Superuser account.


3. Select **Save** when finished.

Once the user is successfully created, the **User** dialog opens for that newly created User.

The screenshot shows a user management interface for a user named 'austin78' with the role 'ADMIN'. The 'DETAILS' tab is selected. The form contains the following fields:

- FIRST NAME:** Text input with 'Austin'.
- LAST NAME:** Text input with 'Texas'.
- EMAIL:** Text input with 'austin78@mail.com'.
- USERNAME:** Text input with 'austin78'.
- PASSWORD:** Text input with a 'SHOW' toggle.
- CONFIRM PASSWORD:** Text input with a 'SHOW' toggle.
- USER TYPE:** Dropdown menu set to 'System Administrator'.

At the bottom right are 'CANCEL' and 'SAVE' buttons.

The count for the number of users has also been updated, and a new entry for the new user is added to the list of users below the edit form. The same window opens whether you click on the user's name, or the Edit (  ) button beside the user. Here, the User's **Organizations**, **Teams**, and **Permissions**, as well as other user membership details, may be reviewed and modified.

## Note

If the user is not a newly-created user, the user's edit screen displays the last login activity of that user. This information persists at the top of the screen regardless of which tab you're viewing.

This screenshot is similar to the previous one but includes a red box highlighting the 'LAST LOGGED IN: 5/6/2019 2:33:27 PM' status at the top of the form. The rest of the form fields and layout are identical to the previous screenshot.

When you log in as yourself, and view the details of your own user profile, you can manage tokens from your user profile. See [Users - Tokens](#) for more detail.

The screenshot shows the user profile for 'austin78' with the role 'ADMIN'. The 'TOKENS' tab is highlighted with a red box. The form includes fields for First Name (Austin), Last Name (Texas), Email (austin78@mail.com), Username (austin78), Password (with a 'SHOW' toggle), Confirm Password (with a 'SHOW' toggle), and User Type (System Administrator). 'CANCEL' and 'SAVE' buttons are at the bottom right.

## 8.2. User Types - Quick View

Once a user has been created, you can easily view permissions and user type information by looking beside their user name in the User overview screen.

The screenshot shows the user profile for 'jdodge' with the role 'AUDITOR'. A red arrow points to the role label with the text 'View user labels here for Auditor, Admin, LDAP, etc.'. The form includes fields for First Name (Josie), Last Name (Dodge), and Email (jdodge@mail.com). 'DETAILS', 'ORGANIZATIONS', 'TEAMS', and 'PERMISSIONS' tabs are visible at the top.

If the user account is associated with an enterprise-level authentication method (such as SAML, RADIUS, or LDAP), the user type may look like:

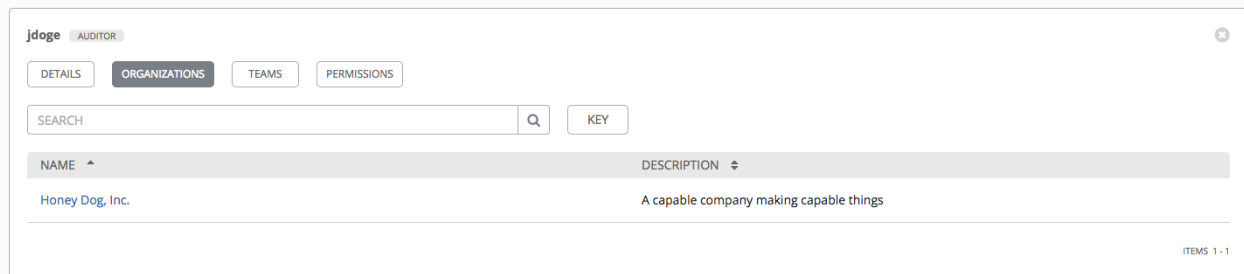
The screenshot shows the user profile for 'jdodge' with the role 'RADIUS'. A red arrow points to the role label. The form includes fields for First Name (Josie), Last Name (Dodge), and Email (jdodge@mail.com). 'DETAILS', 'ORGANIZATIONS', 'TEAMS', and 'PERMISSIONS' tabs are visible at the top.

If the user account is associated with a social authentication method, the user type will look like:

The screenshot shows the user profile for 'jdodge' with the role 'SOCIAL'. A red arrow points to the role label. The form includes fields for First Name (Josie), Last Name (Dodge), and Email (jdodge@mail.com). 'DETAILS', 'ORGANIZATIONS', 'TEAMS', and 'PERMISSIONS' tabs are visible at the top.

## 8.3. Users - Organizations

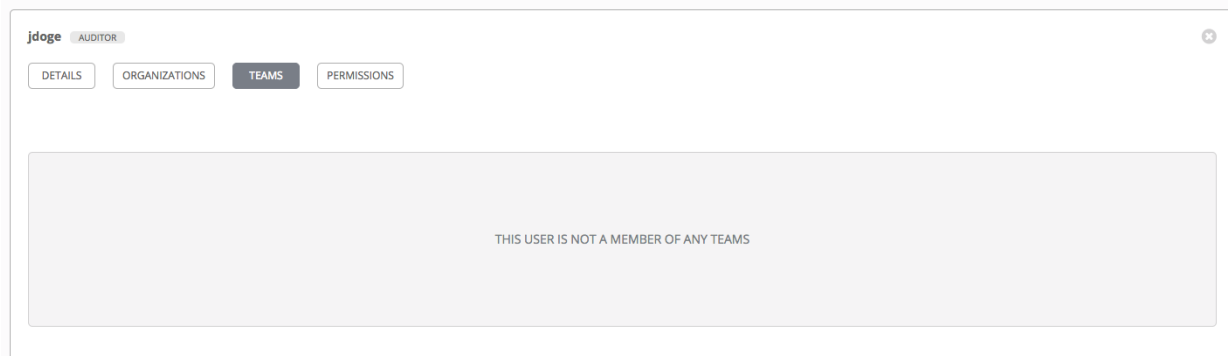
This displays the list of organizations of which that user is a member. This list may be searched by Organization Name or Description. Organization membership cannot be modified from this display panel.



## 8.4. Users - Teams

This displays the list of teams of which that user is a member. This list may be searched by **Team Name** or **Description**. Team membership cannot be modified from this display panel. For more information, refer to [Teams](#).

Until a Team has been created and the user has been assigned to that team, the assigned Teams Details for the User appears blank.



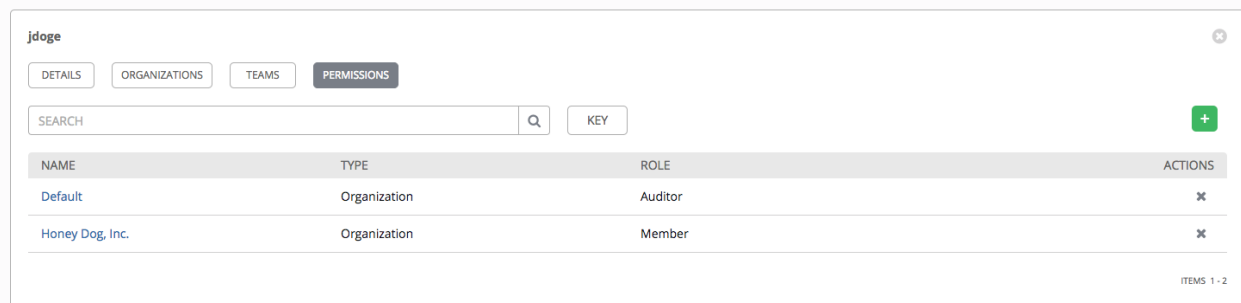
## 8.5. Users - Permissions

The set of Permissions assigned to this user (role-based access controls) that provide the ability to read, modify, and administer projects, inventories, job templates, and other Tower elements are Privileges.

### Note

It is important to note that the job template administrator may not have access to any inventory, project, or credentials associated with the template. Without access to these, certain fields in the job template aren't editable.

This screen displays a list of the roles that are currently assigned to the selected User and can be sorted and searched by **Name**, **Type**, or **Role**.




The screenshot shows the 'Permissions' tab for user 'jdodge'. It features a search bar and a table with columns: NAME, TYPE, ROLE, and ACTIONS. The table lists two roles: 'Default' (Organization, Auditor) and 'Honey Dog, Inc.' (Organization, Member). A green '+' button is in the top right corner.

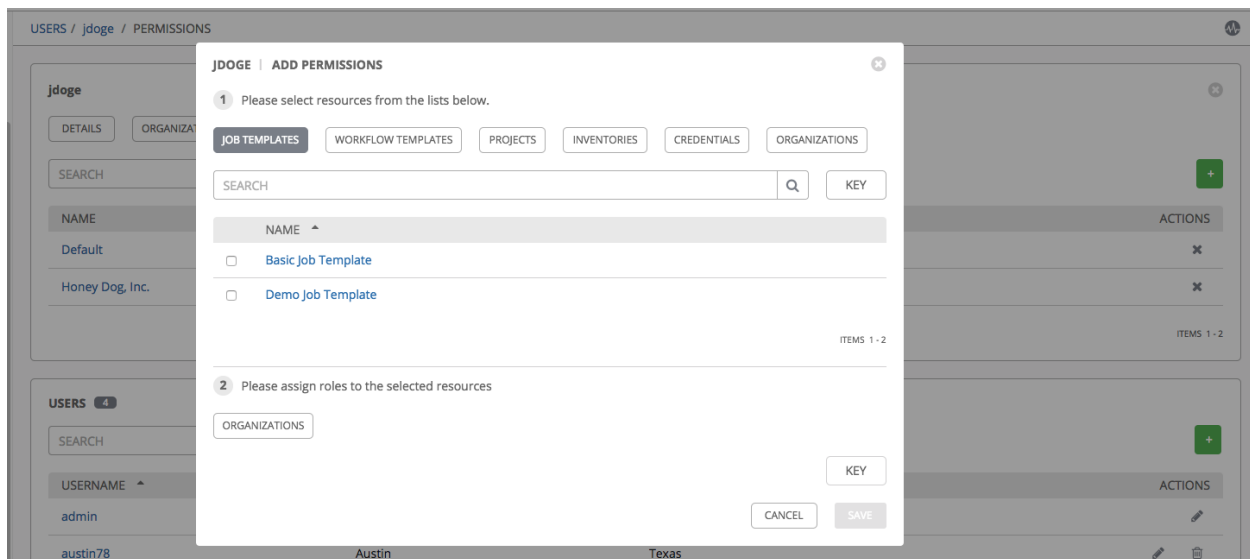
NAME	TYPE	ROLE	ACTIONS
Default	Organization	Auditor	✕
Honey Dog, Inc.	Organization	Member	✕

ITEMS 1 - 2

### 8.5.1. Add Permissions


To add permissions to a particular user:

1. Click the  button, which opens the Add Permissions Wizard.



2. Click to select the Tower object for which the user will have access:
  - **Job Templates.** This is the default tab displayed in the Add Permissions Wizard.
  - **Workflow Templates**
  - **Projects**
  - **Inventories**
  - **Credentials**
  - **Organizations**

## Note

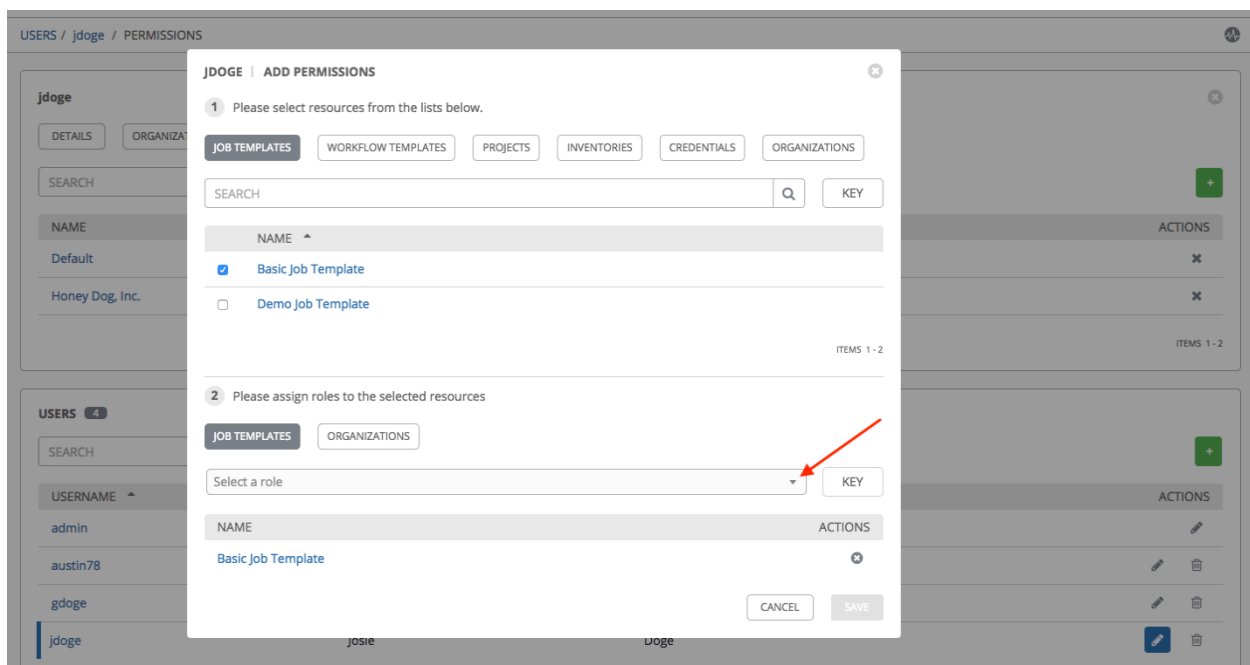
You can assign different roles to different resources all at once to avoid having to click the  button. To do so, simply go from one tab to another after making your selections without saving.

3. Perform the following steps to assign the user specific roles for each type of resource:

1. In the desired tab, click the checkbox beside the name of the resource to select it.

The dialog expands to allow you to select the role for the resource you chose.

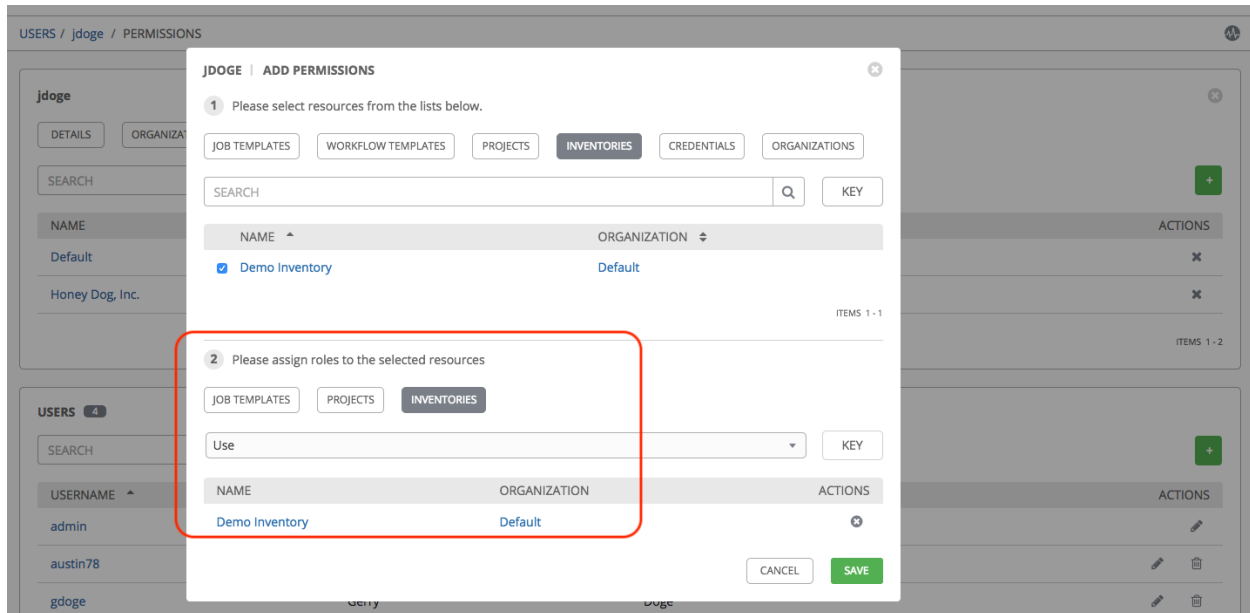
2. Select the role from the drop-down menu list provided. Only some roles are applicable to certain resources.



## Tip


Use the **Key** button to display the help text for each of the roles applicable to the resource selected.

3. Review your role assignments for each of the Tower objects by clicking on their respective buttons in the expanded section 2 of the Add Permissions Wizard.



4. Click **Save** when done, and the Add Permissions Wizard closes to display the updated profile for the user with the roles assigned for each selected resource.

jdoge			
DETAILS	ORGANIZATIONS	TEAMS	PERMISSIONS
SEARCH	Q	KEY	+
NAME	TYPE	ROLE	ACTIONS
Default	Organization	Auditor	×
Demo Inventory	Inventory	Use	×
Honey Dog, Inc.	Organization	Member	×
Sample Project	Project	Admin	×
Basic Job Template	Job Template	Admin	×
ITEMS 1 - 5			

To remove Permissions for a particular User, click the Disassociate (  ) button under **Actions**. This launches a **Remove Role** dialog, asking you to confirm the disassociation.

## Note

You can also add teams, individual, or multiple users and assign them permissions at the object level (projects, inventories, job templates, and workflow templates) as well. This feature reduces the time for an organization to onboard many users at one time.

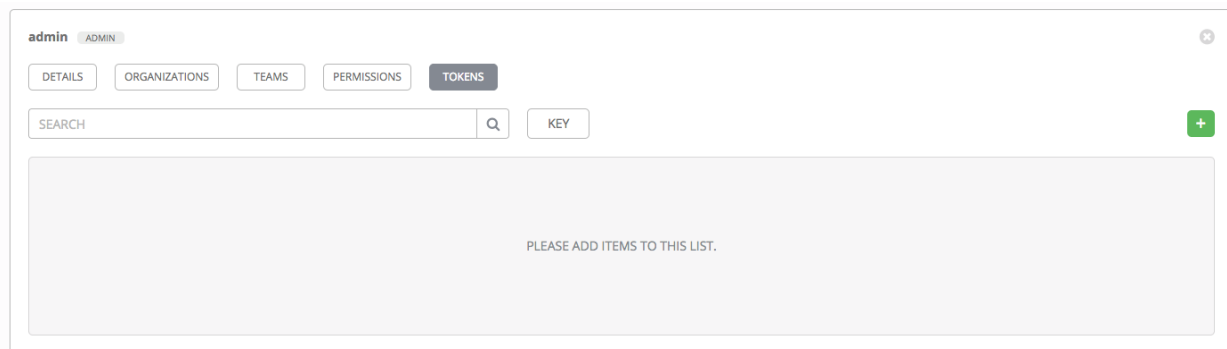
## 8.6. Users - Tokens





The **Tokens** tab will only be present for your user (yourself). Before you add a token for your user, you may want to [create an application](#) if you want to associate your token to it. You may also create a personal access token (PAT) without associating it with any application. To create a token for your user:

1. If not already selected, click on your user from the Users list view to configure your OAuth 2 tokens.
2. Click the **Tokens** tab from your user's profile.

When no tokens are present, the Tokens screen prompts you to add them:



3. Click the  button, which opens the Create Token window.
4. Enter the following details in Create Token window:
  - **Application:** enter the name of the application with which you want to associate your token. Alternatively, you can search for it by clicking the  button. This opens a separate window that allows you to choose from the available options. Use the Search bar to filter by name if the list is extensive. Leave this field blank if you want to create a Personal Access Token (PAT) that is not linked to any application.
  - **Description:** optionally provide a short description for your token.
  - **Scope** (required): specify the level of access you want this token to have.
5. When done, click **Save** or **Cancel** to abandon your changes.

After the token is saved, the newly created token for the user displays with the token information and when it expires.

TOKEN INFORMATION

TOKEN

BxcMz8sIOy2K8I7G4cmAoZ00Q01zq5

REFRESH TOKEN

3zA0gKCmrMFF8dSfhNLOowX93DmiIM

EXPIRES

3/15/3019 4:56:20 PM

OK

## Note

This is the only time the token value and associated refresh token value will ever be shown.

In the user's profile, the application for which it is assigned to and its expiration displays in the token list view.

adminADMINLAST LOGGED IN: 5/28/2019 1:19:56 PM

DETAILS

ORGANIZATIONS

TEAMS

PERMISSIONS

TOKENS

SEARCH

Q

KEY

+

My creds app Token

APPLICATIONMy creds app

EXPIRATION9/28/3018 3:11:51 PM

🗑️

ITEMS 1 - 1

[Next](#) [Previous](#)