Adding and Managing Users

Provided you have System Administrator privileges, you can add users to your environment and manage their properties, including their passwords and permissions.

Note that adding a user to your environment does not automatically provide him/her access to any transactions. To access any transactions, a user must either be provided some Administrative Role that provides general app access (we'll cover how to do this below) or be assigned as a participant of a specific transaction.

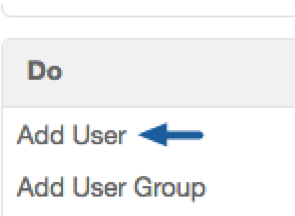
This tutorial will cover how to add a user, how to view a list of all the users in an environment and manage his/her properties, and how to provide users with Administrative Role permissions.

Adding a New User

Adding a new user stores a person's name and email address in your environment and sends a notification to him/her with a link to set a login password.

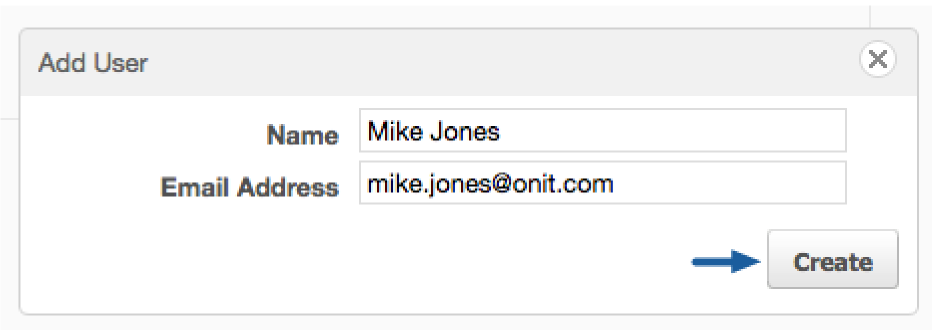
1. Browse to Add User

Browse to your environment's **Administration** page and select **Add User** from the left-hand pane.



2. Provide the User's Details

In the **Add User** dialog, provide your new user's **Name** and **Email Address** and select **Create**.

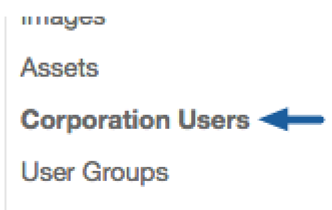


That's all there is to adding a user. The user should now receive an email with a link to create his/her password for logging into your environment.

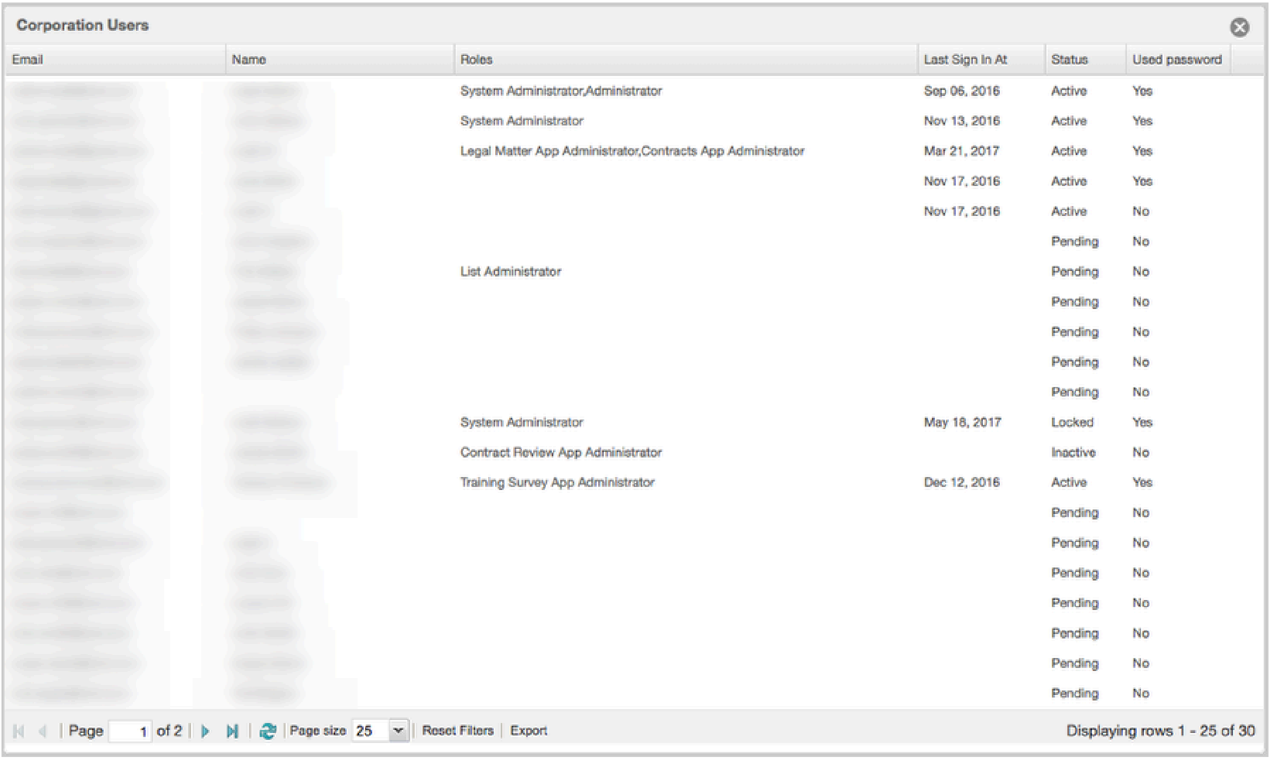
Note: As mentioned above, adding a user does not automatically grant him/her access to any transactions.

Viewing Your Environment's Users

To view all the users associated with your environment, select **Corporation Users** from the left-hand pane of your **Administration** page.



From this list, you can see a user's status (active, pending, or deactivated) and last sign-in date.


Corporation Users

Email	Name	Roles	Last Sign In At	Status	Used password
		System Administrator,Administrator	Sep 06, 2016	Active	Yes
		System Administrator	Nov 13, 2016	Active	Yes
		Legal Matter App Administrator,Contracts App Administrator	Mar 21, 2017	Active	Yes
			Nov 17, 2016	Active	Yes
			Nov 17, 2016	Active	No
				Pending	No
		List Administrator		Pending	No
				Pending	No
				Pending	No
				Pending	No
				Pending	No
		System Administrator	May 18, 2017	Locked	Yes
		Contract Review App Administrator		Inactive	No
		Training Survey App Administrator	Dec 12, 2016	Active	Yes
				Pending	No
				Pending	No
				Pending	No
				Pending	No
				Pending	No
				Pending	No
				Pending	No

Page 1 of 2 | Page size 25 | Reset Filters | Export | Displaying rows 1 - 25 of 30

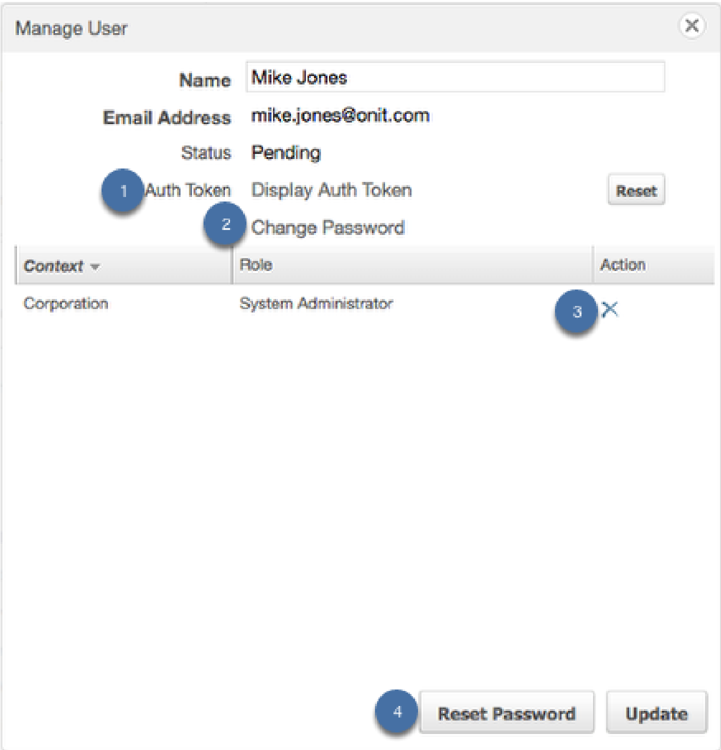
You'll also see a column called **Roles**, which displays any Administrative Role/s a user has been provided.

Note: Administrative Roles are different than the Roles you may be familiar with creating in the **Wizard** and using on a Record-specific basis.

Administrative Roles have to do with a user's permissions across your environment; You can read about Administrative Roles in the Admin Roles section of [Crash Course on Security](). We'll also show you how to add Administrative Roles to a user in the next section of this tutorial.

Click on one of your users in this list to open a dialog where you can:

1. View or reset the user's authentication token,
2. Change his/her password,
3. Remove his/her Administrative Roles, or
4. Reset his/her password



Change Password vs Reset Password

Note that there's a difference between changing someone's password for them and reseting someone's password.

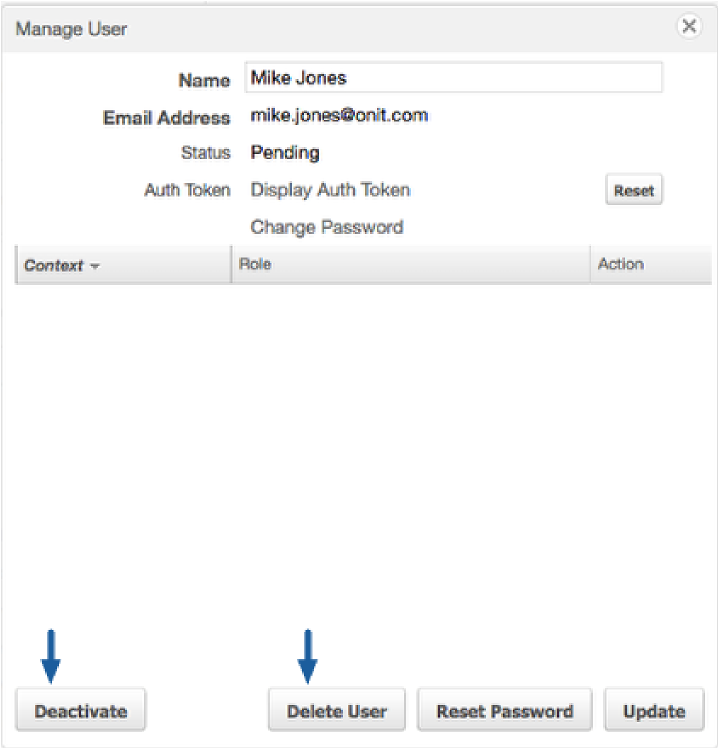
You can set a user's password yourself with the **Change Password** property. To do so, select **Change Password**, enter the new password value and select **Update**.

If you want to prompt a user to reset his/her own password, select **Reset Password**.

When a user does *not* have any Administrative Roles assigned to him/her, you will also see a **Deactivate** button and a **Delete User** button.

Selecting **Deactivate** will prevent a user from being able to log into your environment or access its Records.

Selecting **Delete User** will delete a user from your environment completely. However, you may not delete a user if he/she is a participant on *any* Record in the environment.



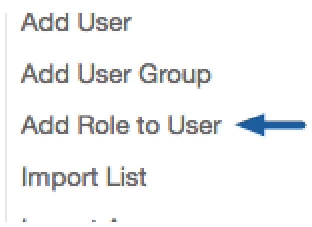
Providing Users with Administrative Roles

From your **Administration** page, you can also provide a user with one or more Administrative Roles, which are used to provide a user permissions across an entire corporation or app.

You can read about the different types of Administrative Roles in [Security Layer: Admin Roles]Crash Course on Security.

1. Browse to Add Role to User

To assign an Administrative Role to a user, browse to **Add Role to User** from the left-hand pane of your environment's **Administration** page.



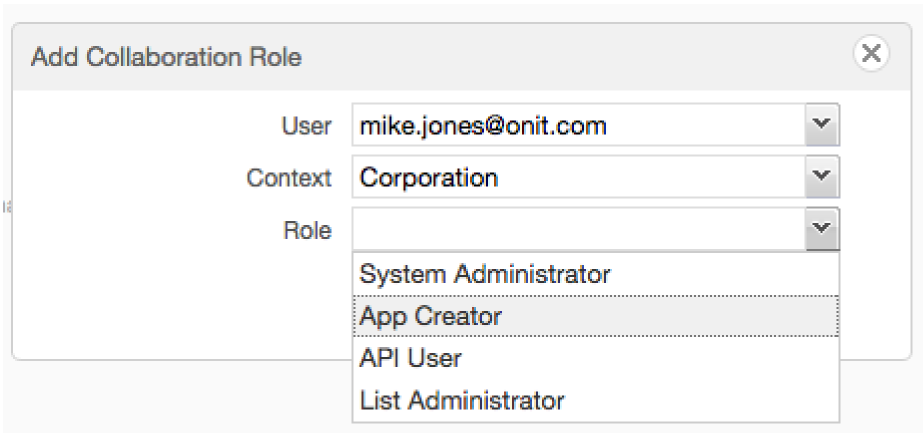
2. Configure the User's Admin Role

From the **User** dropdown, select an existing user.

Inside the **Context** dropdown, select the context you want to grant your user permissions to. You'll see two *types* of options:

- **The name of every App:** If you want to assign the user an **App Administrator** role, (which applies exclusively to a specific App), select an App.
- **Corporation:** If you want to assign any other Administrative Role, (which will apply to the entire corporation), select this option. (You'll find **Corporation** as the very last value in the dropdown.)

Finally, select the **Role** type. Reference the Administrative Role table in our Crash Course on Security tutorial to find the set of permissions that fits your needs.



Select **Ok** to save your changes.

Wrapping Up

That's all there is to managing the basic properties of your environment's users. Remember that adding a user to your environment doesn't automatically grant him/her access to any Records or permissions to do anything inside your environment. We recommend checking out our Crash Course on Security article to start understanding how to let your users to do more once they've been added to your environment.