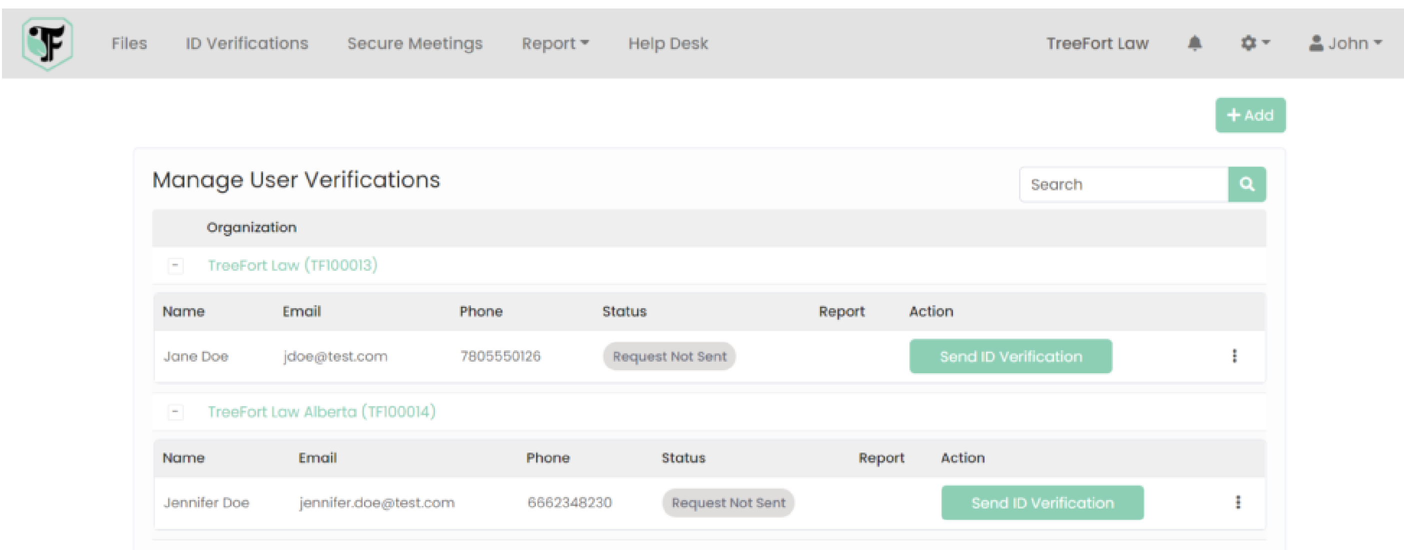
Managing Users

Administrators for an organization or suborganization are able to manage users, including adding new users to TreeFort and editing user information. **Note:** an administrator for the entire organization will be able to manage users for the organization and all suborganizations, however an administrator for a suborganization will only be able to manage users for their suborganization. More information on creating and managing suborganizations can be found here.

Before a user can be created for your organization or suborganization, the user will have to go through the same ID verification process that your clients experience in order to prove their identity and become a verified user within TreeFort. To create a new user or manage existing ID verification requests, navigate to the **Administrative Settings** option in the navigation bar and select **Manage User Verification Requests**, as shown below.

You will be directed to the following page, where you will be able to see all existing ID verification requests for users at your organization or suborganization.



Create a New User

Once you have navigated to the **Manage User Verification Requests** tab, as shown above, you can add a new user by selecting the **+ Add** button, which will open a popup allowing you to enter the information required to create a new user, as shown below.

You will be prompted to enter the following information to create a new user. **Note:** this is mostly the same information that is required to create a new client.

Name: you must enter a first name and last name for a user, however the middle name field is optional. If the user has only one name, select the **Client only has one name** checkbox.

Address: you must enter the user's street address, city, province, country, and postal code. **Note:** this address will be compared against the user's government-issued photo ID (e.g. driver's license or passport), and with other reliable sources (e.g. an account they hold at a financial institution). Therefore, the address entered here should be the same address as found on their government-issued photo ID and associated to their account with their financial institution.

Email Address: you must enter the user's email address. This email address will be used to send the user a link to begin the ID verification process, and will also be used for any subsequent notifications and communications sent to the user. **Note:** if your organization or suborganization has set up restricted domains from your organization or suborganization settings (e.g. users must have @treefort.tech email addresses), you must enter an email address that conforms to the domain restrictions in order to save the user.

Phone Number (cellphone): you must enter the user's cell phone number. The user must have access to a cell phone with a camera and the ability to receive SMS messages, as security codes will be sent via SMS to the user, and the user will be required to take photos of their government-issued ID and complete a face scan using the camera on their cellphone.

Organization: you must select which organization or suborganization a user will be associated to from a dropdown of available organization / suborganizations.

Jurisdiction: you must select which jurisdiction the user is associated with. This field determines the applicable legislation that will be referenced in the final TreeFort ID Verification Reports for all ID verification requests sent to clients that were initiated by this user. For instance, if the "Law Society of Alberta" is selected, all ID verification reports for clients that were initiated by this user will reference the applicable Law Society of Alberta Model Client ID Rules. The user will be able to change their jurisdiction at any time from their user settings. **Note:** custom codes can also be created for your organization to reference other applicable legislation, or to not reference any specific legislation at all. If you require a custom code for your organization, please contact us at **support@treefort.tech**.

Note that date of birth is not a required field, as the user's date of birth will be pulled from their government-issued ID during the ID verification process.

When you are finished entering your user's information, select **Save** to add your user to the file. Once created, the user will appear in the list of existing ID verification requests under the organization or suborganization that was selected for that user, as shown below.

Initiating an ID Verification

Once the user has been added to the **Manage User Verifications** page, you can initiate the ID verification process with the user by selecting the **Send ID Verification** button next to the user you want to send the ID verification request to, as shown below. Once selected, a popup will display asking you to confirm that you want to send an ID verification request to the selected user. If you want to proceed, select **Ok**. the status for that user will change from **Request Not Sent** to **Pending**.

Cancelling an ID Verification

Once the request is sent, the user will have a **maximum of 3 days** to complete the ID verification process. If the user does not complete the process within 3 days, or if an administrator at your organization cancels the ID verification request prior to completion by selecting the **Cancel ID Verification** button from the **Action** column of the user table, as shown below, the user status will change to **Cancelled**. You can reset the ID verification and re-initiate the ID verification process by selecting **Reset ID Verification**.

Editing an ID Verification

If you want to edit a user's information that will be used in the ID verification process (e.g. some information was entered incorrectly, the user's information has changed, etc.), you can edit the user's information by selecting the **edit** icon beside the user you want to edit and selecting the **Edit** option, as shown below. Selecting this option will open a popup allowing you to edit any user information. When you are finished editing information, select **Save** to save the updated user information.

The User Experience

Once the ID verification process has been initiated by an administrator at your organization or suborganization, the user will receive an email with a link to begin the ID verification process. **Note:** this process is the same as the process that a client would experience when completing an ID verification request. A full step-by-step walkthrough of the user experience for the ID verification process can be found in the article titled **The ID Verification Process** under **The Client Experience** (section 2).

Viewing the TreeFort Report

Once the user has completed the ID verification process, the individual who initiated the ID verification process with the client (an administrator at your organization or suborganization) will receive an email and a notification within the TreeFort application indicating that there is a report available for review for that user.

To view the TreeFort Report for a user, navigate back to the **Manage User Verifications** tab in the **Administrative Settings** option from the top navigation bar. If a report is available for review, the user status will be set to **Review Report**, and the download icon will be available for selection in the **Report** column next to the user. To download the report to your computer, select the download icon, as shown below.

Once the report is downloaded, you can review the report to determine if you want to "Approve" or "Reject" the ID verification for that user. More information on reading the TreeFort report can be found in the article titled **Understanding the TreeFort Report**. If you select to "Approve" the user, they will be created as a new user in TreeFort, and will receive an email to begin the account creation process. More information on the process a user will take to create their account can be found **here** under the **Creating Your Account** section (section 3). By selecting to **Approve** a user, the user will be removed from the **Manage User Verifications** tab, and will appear in the list of verified users in the **Manage Users** tab, which is explained later in this article in the **Manage Users** section.

User Roles

Before being approved, the administrator must select a role for the user at their organization or suborganization, as shown below. The available user roles are:

Admin – If the user is being selected as **Admin** for the entire organization, they will have **Administrative Settings** visible in the top navigation bar, and will be able to manage their organization’s information. They will be able to edit organization settings, manage billing and subscription information, and will also manage their organization’s user access by creating, approving, editing, and removing users. They will also be able to manage their suborganizations, as well as suborganization users, if applicable. An **Admin** for an organization will also have full access to the Reports section for all users and suborganizations, as the **Accounting** user does. If the user is being selected as **Admin** for a suborganization, they will have the same functionality as an **Admin** for the entire organization, however they will manage the suborganization’s information (general settings and managing users for their suborganization only). Suborganization Admins will have full access to the Reports section for all users associated *only* with their suborganization.

Regular User – this is a traditional user role within TreeFort. **Regular Users** will be able to manage their own account settings, manage files and clients, initiate ID verification requests, etc.

Accounting – this role will only have access to view the Reports section within TreeFort. They will be able to filter reports for any user within the organization, or all users. If the **Accounting** role is applied to a user associated with the entire organization, they will have access to reports for the entire organization, however if applied to a user associated to a suborganization, they will only have access to reports for suborganization users.

Manage Users

Verified users (i.e. users who have been “approved” from the **Manage User Verifications** tab after going through the ID verification process) will appear in the **Manage Users** tab, sorted according to the organization or suborganization they are associated to. To view to the **Manage Users** tab, navigate to the **Administrative Settings** option from the top navigation bar and select the **Manage Users** option, as shown below.

The following page will be displayed, showing all existing users separated according to the organization or suborganization they are associated with. In the following example, the newly created user John Doe is associated to the suborganization **TreeFort Law Alberta**, and there are additional users under the other suborganization **TreeFort Law British Columbia**, as well as under the entire organization **TreeFort Law**.

Note: if a user at your organization has forgotten their **Account Number** required to login, this number will be shown next to the organization or suborganization they are associated with. For example, in the below screenshot, the **Account Number** associated with users of TreeFort Law Alberta would be TF100014.

Editing Users

If you want to edit a user's information for any reason (e.g. some information was entered incorrectly, the user's information has changed, etc.), you can edit the user's information by selecting the **edit** icon beside the user you want to edit and selecting the **Edit** option, as shown below.

Selecting to **Edit** a user will open a popup allowing you to edit most user information, including the user's role. When you are finished editing information, select **Save** to save the updated user information.

Note: although most user information can be edited, a full audit trail of all information that has changed over time for a user is recorded and available to view. More information on the user information audit trail can be found in the next section of this article.

User Information Audit Trail

User information can be edited by administrators from the **Manage Users** tab, however a full audit trail of all information that has changed over time for each user is recorded and available to view. To view the audit trail for a specific client, select the **edit** icon beside the user you want to view and select the **Audit Trail** option, as shown below.

This will open a popup displaying a full list of every change that has been made to a user's information over time, as shown below.