PCMIMS+ Administration & Configuration Guide

April 2025

How it Works: The Building Blocks

Primero is a case management information management system that allows for data entry and reporting for child protection (CPIMS+), gender-based violence (GBVIMS+), and protection case management (PCM). The system helps intake relevant information via multiple sources, consolidates the information into relevant record types (Cases / Incidents) and allows service providers to report and make educated decisions to assist in these locations.

Records

Primero uses three types of "records" to represent protection-related information:

- **Case (for CPIMS+, GBVIMS+ and PCMIMS+)** - This represents an individual beneficiary.
- **Incident (for CPIMS+ and GBVIMS+)** - This represents an event that has occurred. This is often an incident of violence or an encounter with the beneficiary outside of the typical case management process.
- **Tracing Request (for CPIMS+)**- This represents an individual seeking to be reunified with one or more unaccompanied or separated children. Tracing Requests are used primarily in Family Tracing and Reunification programming.

Each of these three "record types" will contain a different set of information, depending on the system's configuration, and which Primero Modules are in use.

Users

Primero **Users** are the individuals working for service-providing organizations and agencies who use the system.

User Groups

User Groups represent teams of users working together.

For example in CPIMS+, there may be a team of social workers in a particular district providing services to children. There may be another team responsible for the child's best interest determination. A manager of a user group will have some level of access to all of the data managed by that group, but not to the data managed by a different group.

For example in GBVIMS+, there may be a team of GBV Case Workers in a particular district providing services to survivors of GBV. There may be a GBV case management supervisor who needs to review safety plans to ensure effective case management. The case management supervisor of a user group will have some level of access to all of the data managed by that group, but not to the data managed by a different group.

For example, in PCMIMS+, there may be a team of protection caseworkers in a particular district providing services to individuals facing protection risks, such as persons with disabilities or older persons at risk. There may also be a protection case management supervisor who is responsible for ensuring quality case management, including reviewing risk assessments and case plans. The case management supervisor of a user group will have some level of access to all of the data managed by that group, but not to the data managed by a different group.

Roles

Users will have a **Role**, which defines what particular users are allowed to do: for instance viewing records, editing records, creating reports, or configuring the system. Examples of roles in CPIMS+ are Social Worker, CP Manager, and CP Administrator.

Along with defining what actions the user is allowed to perform, roles also limit what kind of information is visible about individual records for a specific user. For example, a CP Social Worker may be allowed to view and edit personally identifiable information (such as name, age, and sex) about a particular client, while a CP Manager may only see a reduced set of information about that same person (age and sex, but not the name), and may not be allowed to edit any of it.

Examples of roles in GBVIMS+ are GBV Case Worker, GBV Case Management Supervisor, and GBV Organization Focal Point. Examples of roles in PCMIMS+ are PCM Caseworker, PCM Case Management Supervisor, and PCM Coordinator/Manager.

Along with defining what actions the user is allowed to perform, roles also limit what kind of information is visible about individual records for a specific user. For example, a GBV Case Worker may be allowed to view and edit personally identifiable information (such as name, age, and sex) about a particular survivor, while a Case Management Supervisor may see the case and incident record for that same person but may not be allowed to edit any of it.

The general term for these limits to what the user can do and what a user can see is *authorization*.

Fields

A **field** (data field) is information within a record. Fields are attributes like name, age, date of birth. Sometimes one field can be used to store several values like a list of protection concerns or all the languages spoken. Fields types include:

- Text Field
- Text Area
- Date
- Date-Time
- Date Range
- Tick Box
- Select Drop Down
- Multi-Select
- Radio Button
- Numeric Field
- Tally Field

Each of these field types is defined in the **Form and Field Configuration** section of this guide.

Forms

A **Form** contains a set of fields for a record. By configuring the Primero application, you can specify new fields on a form, reorder the fields, or allow different forms to share the

same field. In general, fields are organized into forms which represent steps in the user's workflow. For instance, an administrator may add the "Risk Level," and "Protection Concerns" fields to a "Preliminary Assessment" form on the Case record, since case workers collect both these pieces of information during the Preliminary Assessment step of the case management process.

Form Groups

Form Groups appear in the form navigation menu on the left side of the screen when a user is creating, viewing, or editing a record. When a user clicks a form group, it expands or collapses to either show or hide the forms it contains.

For example, in CPIMS+, the "Registration" form group might contain the forms "Child's Details," "Care Arrangements," and "Interview Details." Form Groups keep the form navigation menu organized.

For example, in GBVIMS+, the "Record Information" form group when creating, viewing or editing cases, might contain the forms "Record Information," "Approvals," and "Incidents." Form Groups keep the form navigation menu organized.

For example, in PCMIMS+, the "Record Information" form group when creating, viewing or editing cases, might contain the forms "Record Information," "Intake Assessment," "MHPSS," and "Case Plan" Form Groups keep the form navigation menu organized.

Getting Started

Where to Make Configuration Changes

It is recommended that configuration design take place on a separate sandbox or "demo" instance. This will buffer live end-users from experiencing potential errors from misconfigured forms and roles. Once the configuration has been successfully modified, it can then be applied to production as an import of the Configuration. For more information on how to send configuration from a sandbox or "demo" site to a production site, please see the **Managing Configurations** section of this guide.

Sequencing Configuration Work

Some elements of Primero configuration depend on others. For this reason, we recommend configuring your system in the following order:

1. **Forms and Lookups:** Decide which forms contain which information. Creating Forms is necessary to specify each Role's Form access. In addition, you must

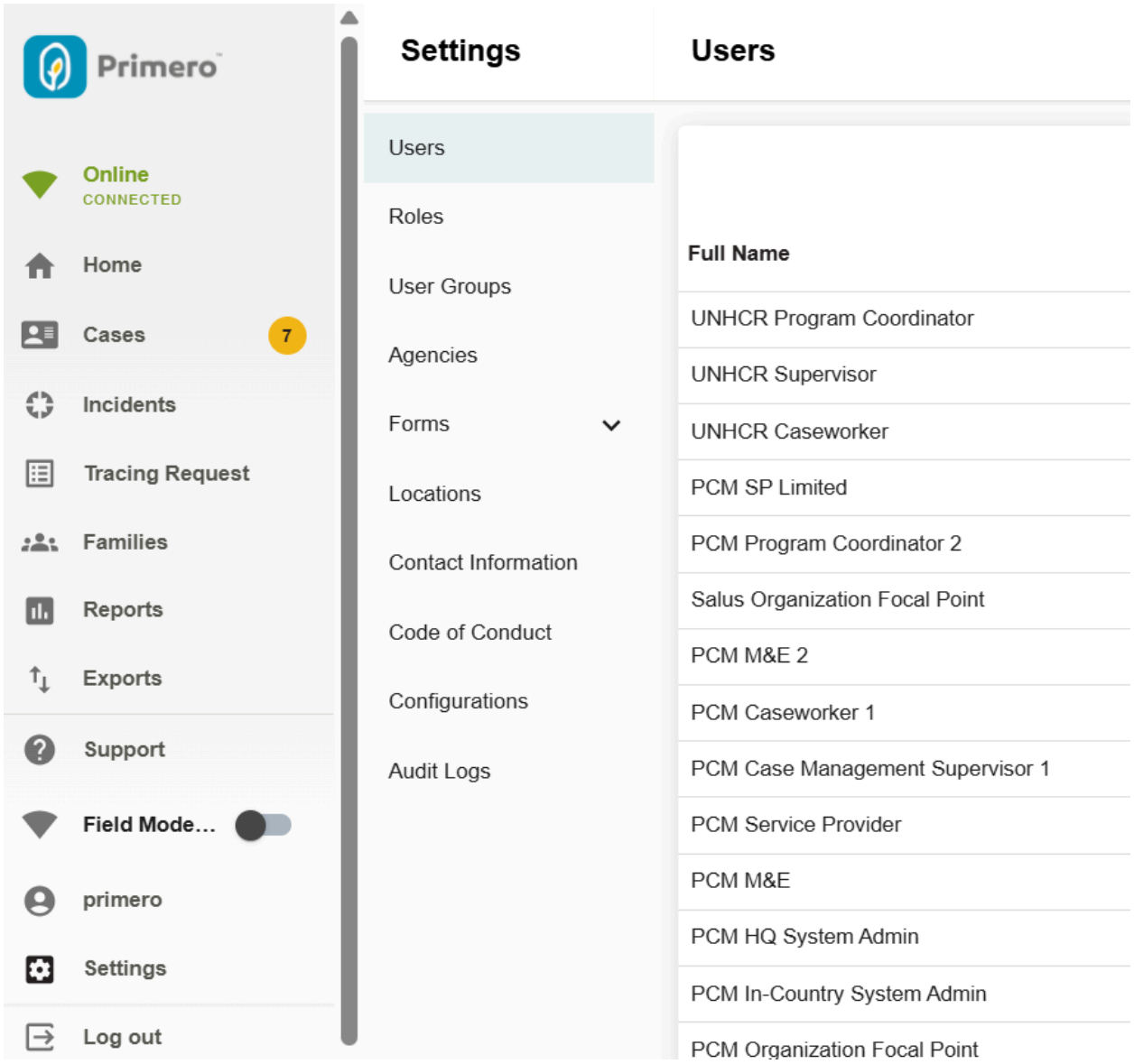
specify options for the “Service Type” lookup before you can set the Service configuration for Agencies and Users.

2. **Agencies, User Groups, Roles:** All of these must be configured before you can create Users.
3. **Users:** While you can create User accounts to test your configuration, you should avoid creating production users until implementation partners have fully reviewed and approved the rest of the configuration. End-users will be added to the production site, as this is the site they will use for data entry.
4. **Reports:** You can begin configuring Reports any time after configuring your Forms, but administrators are recommended to be the users that continue creating and updating Reports after go-live, as any report created is applied for all agencies.

Note: You can configure the **Contact Information** at any point.

Navigating Settings

To begin configuring Primero, click on the **Settings** link in the navigation menu.



Note that both “Forms” and “Lookups” can be found in the “Forms” section of the Settings navigation menu.

Form and Field Configuration

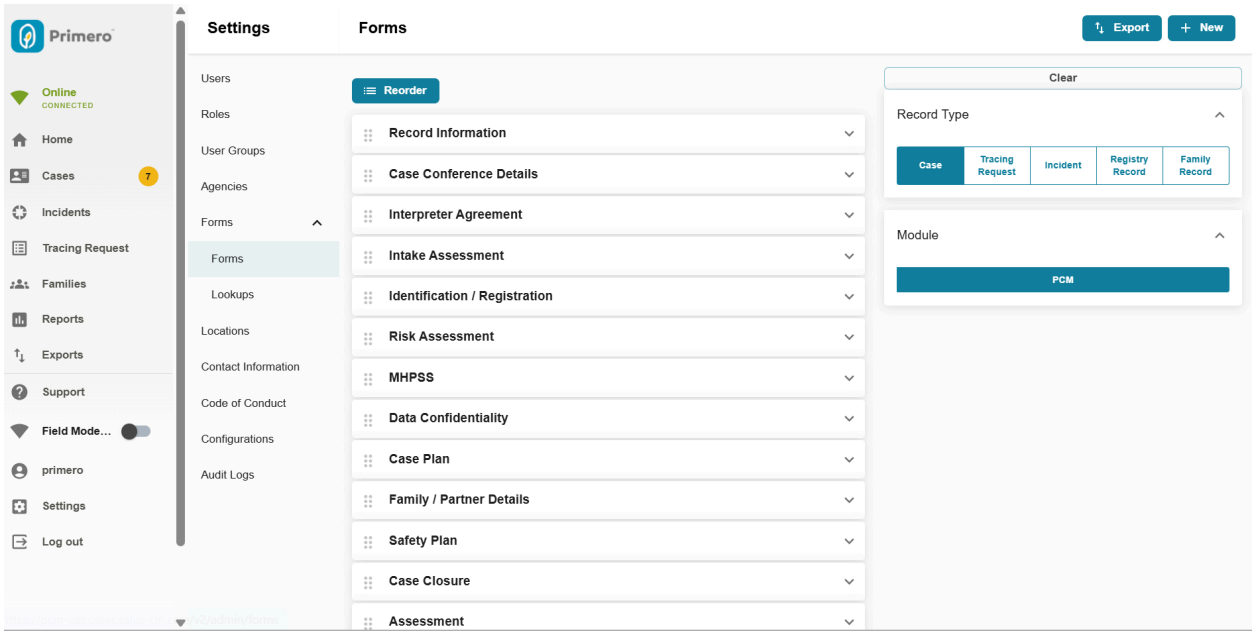
Forms determine how information is organized in Primero and help control which users can see which types of information about a record.

A **Form** contains a set of fields for a record. As an administrator in Primero, you can create a new form, modify the existing forms, specify new fields on a form, reorder the fields, or allow different forms to share the same field.

A **Field** (data field) is information within a record. Fields are attributes like name, age, date of birth. Sometimes one field can be used to store several values like a list of protection concerns or all the languages spoken. The same field can be 'shared' on different forms so that you can enter a date of birth on one form and see it on multiple forms.

The Forms List

To configure Forms, first click on the "Forms" section within the Settings navigation menu, then click the "Forms" link that appears.

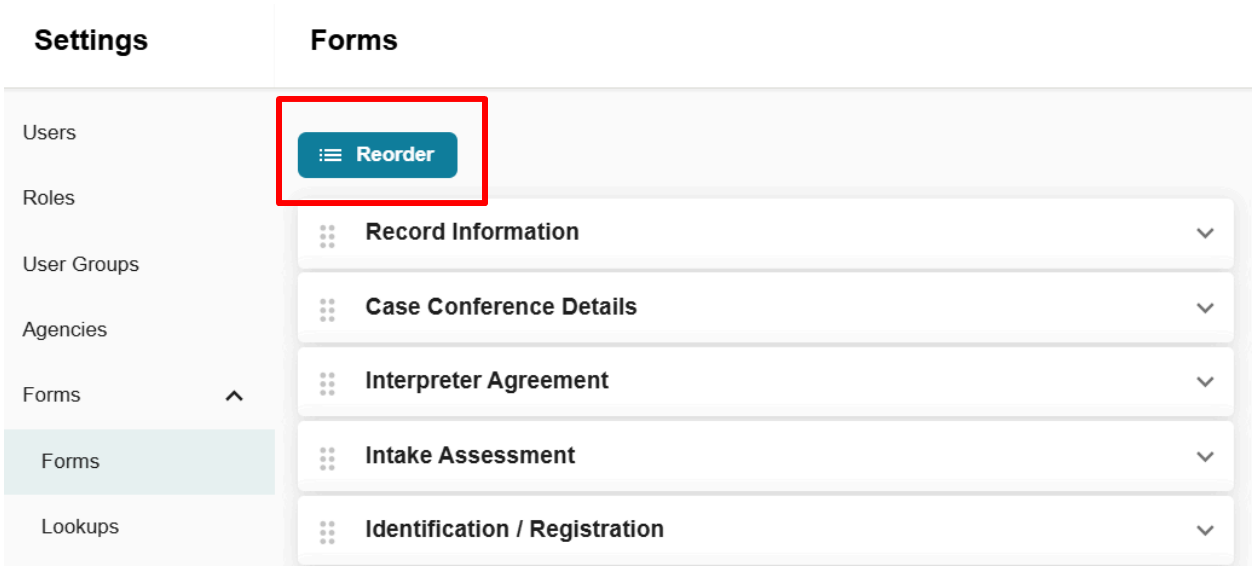


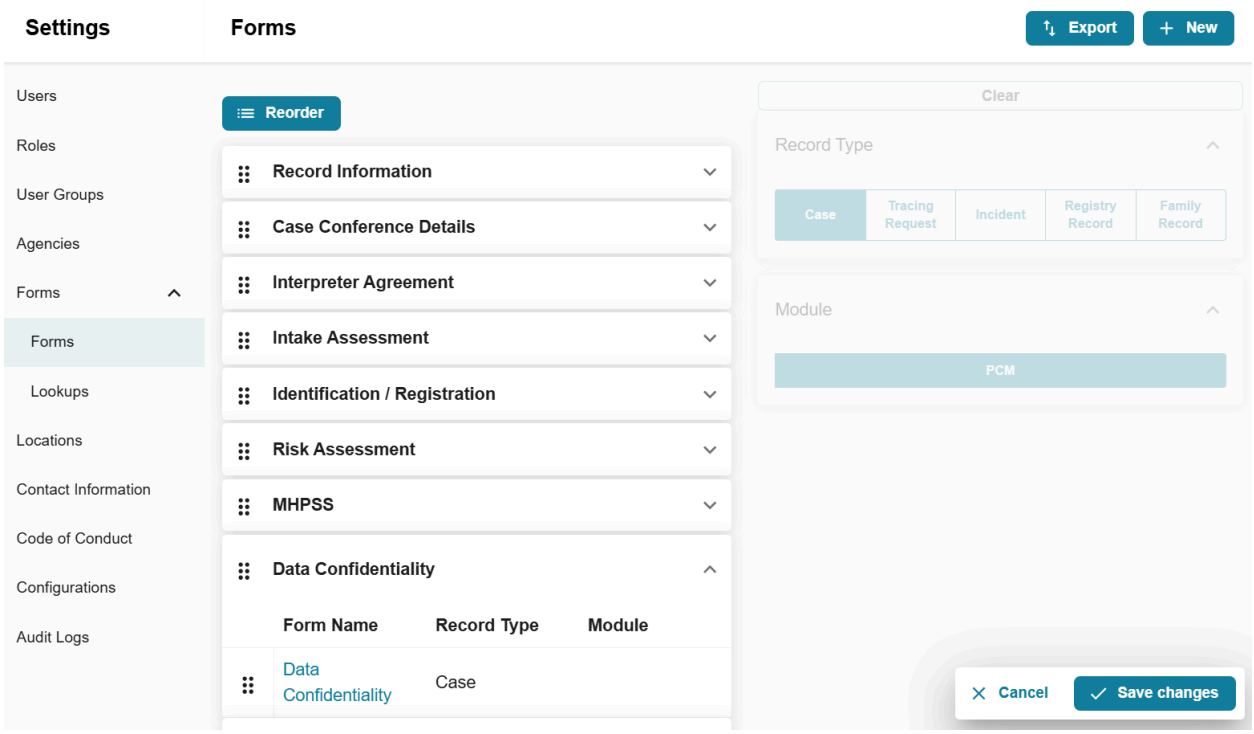
Here, you will see Forms organized by Form Group. Click on a Form Group to expand it and see the forms contained within.

Note that this list only shows Forms for a given Module and Record Type at a given time (e.g. CP Cases, GBV Cases or PCM Cases). You can use the filters on the right side of the page to change which Forms you are viewing.

Reordering Forms

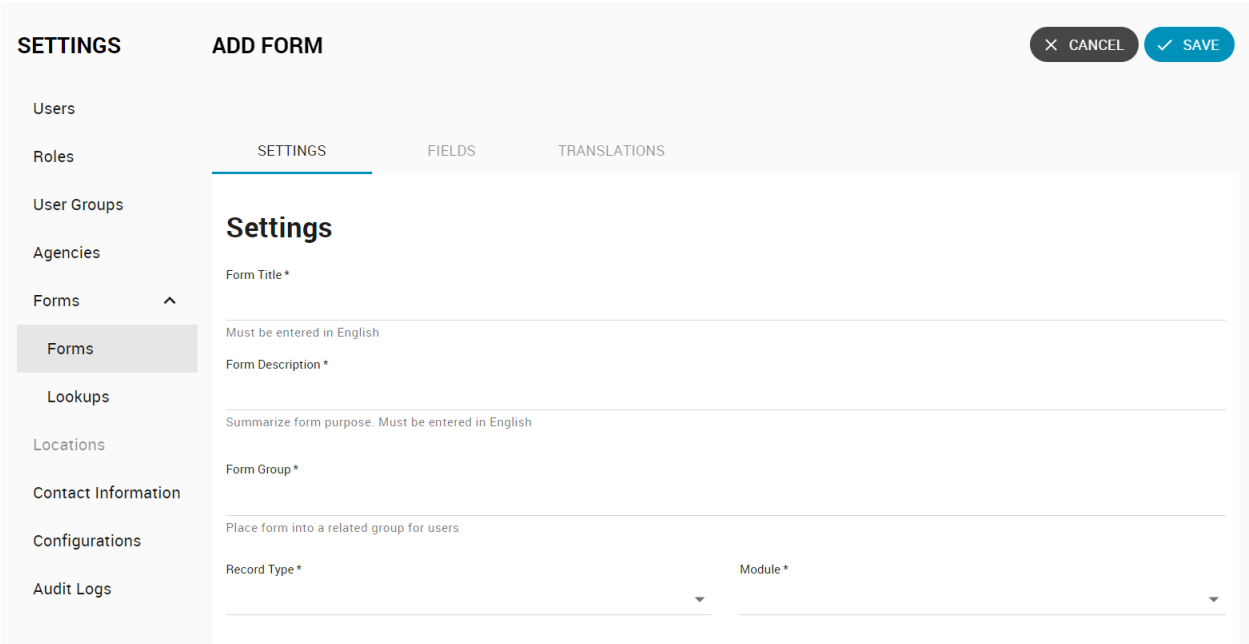
To update the order in which Forms appear, click the "Reorder" button at the top of the list. Then drag and drop Forms and Form Groups into the desired order. Click the "Save Changes" button once you are finished.





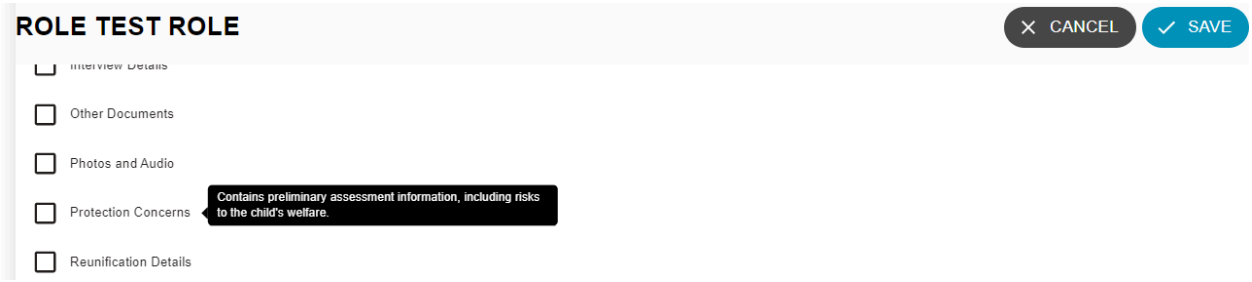
Creating a Form

To create a new form, click the “New” button at the top of the Forms List.

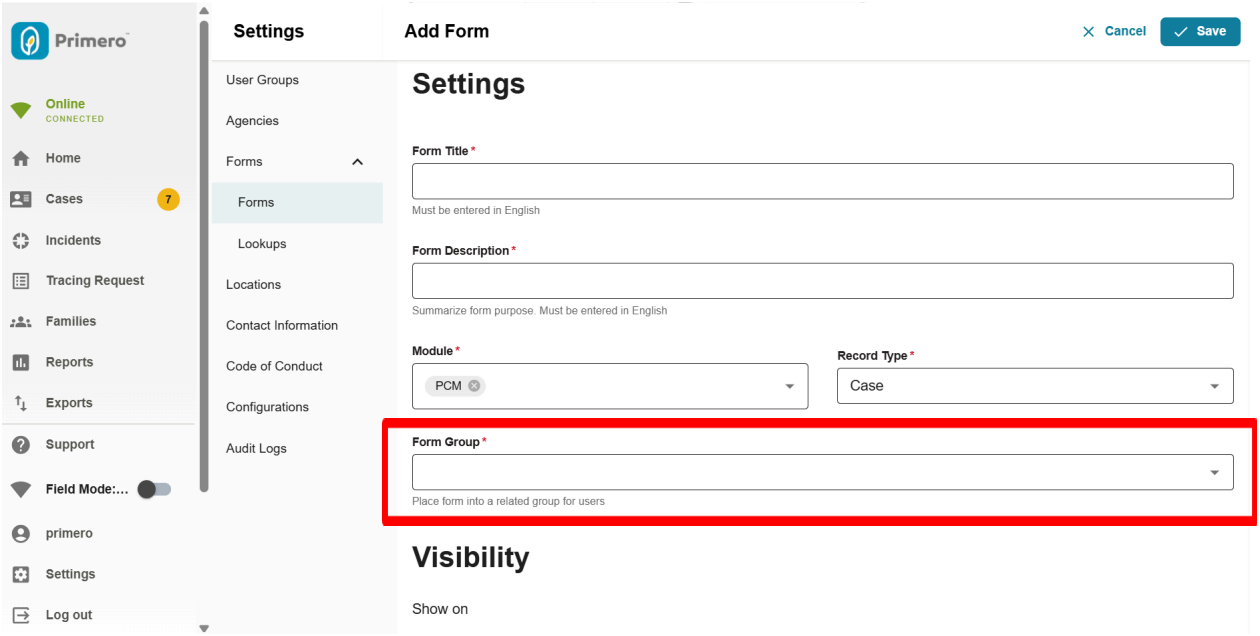


Fill in the following information about the form:

- **Form Title** - This is the name of the Form that will appear in the List of Forms in the Left Navigation panel.
- **Form Description** - This a description of the form. Later, when you are configuring which Forms a Role can access in the Role form, hovering your mouse over the Form name will reveal this Description, to remind you what information you included in this Form, and how it is used.



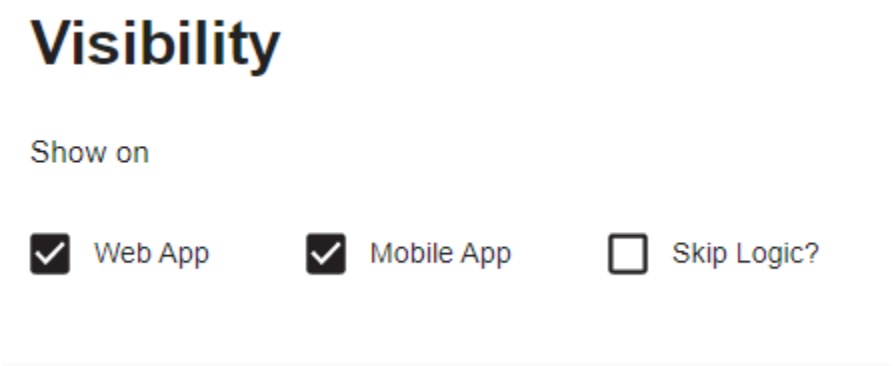
- **Form Group** - This is the name that displays in the Left Navigation Panel at the top level when forms are grouped. The Form Group has a dropdown carrot to the right of the name in the Left Navigation Panel. Clicking on this carrot expands or contracts the Form Group. To add the Form Group Name, you can select an existing Form Group from the dropdown list or add a new one. To add a new one, type the desired name in the box directly below the field and then click on the phrase ‘Click to add <form group name>’ directly below that:



If you create a new form group for your form, it will appear later in one of the Form Group lookups. You will be able to edit and provide a translation for your form group there. For more information on how to edit form groups, see the section **Managing Form Groups**.

If you want the form to appear by itself and not as part of a Form Group, you must enter your Form's name in the Form Group Name field, then click the option to create a new Form Group with this name.

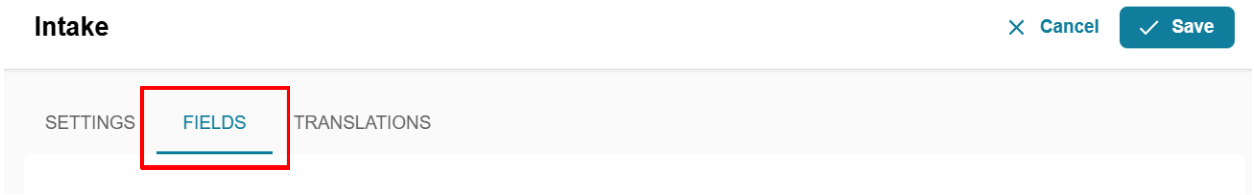
Be sure to specify whether your form is visible.



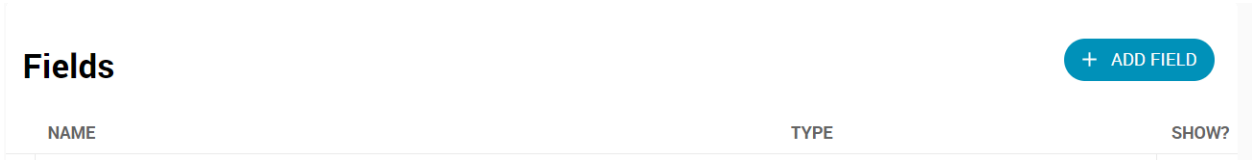
Press the **Save** button when all the desired information is entered.

Adding and Updating Fields

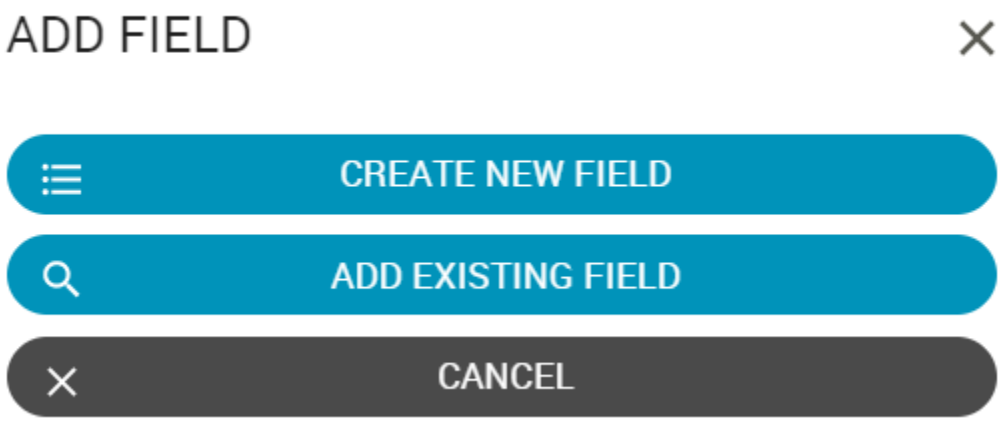
You must create and save a Form before you are able to add fields to it. Once you have saved the Form, click the "Fields" tab.



Here, you can add, update, or reorder any fields in this form.



To add a field to the form, select the ADD button. The following will appear:

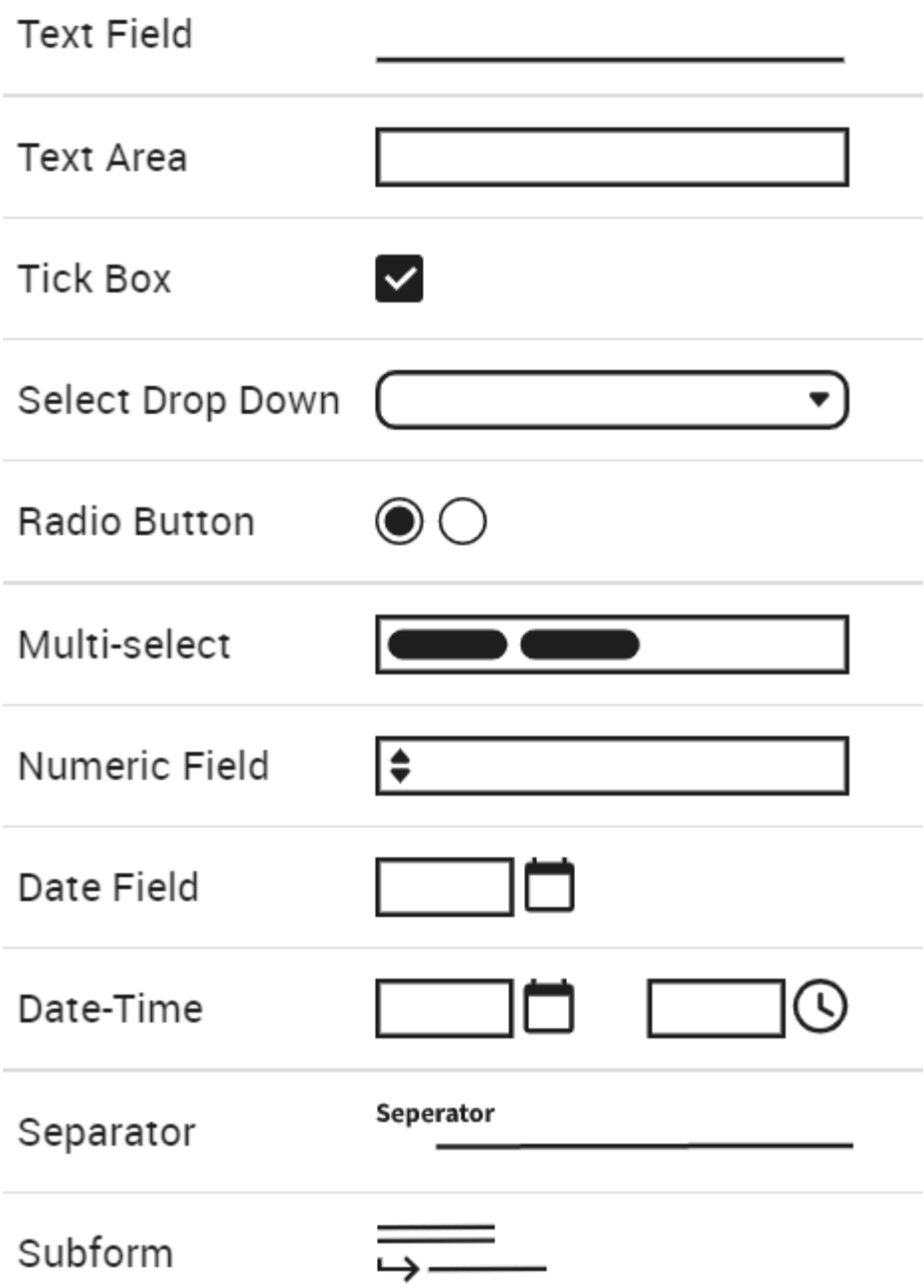


You have two options:

- **Create New Field**: This will create a completely new field on the form. You will get to choose the type of field as well as its options.
- **Add Existing Field:** This will copy an existing field from a different form onto this form. When a user is updating a record, if they enter a value on this field in the first form, the same value will appear automatically on the copied field in the second form. If you choose this option, you will not be able to choose a field type, and you will not be able to update all of the field's configuration options.

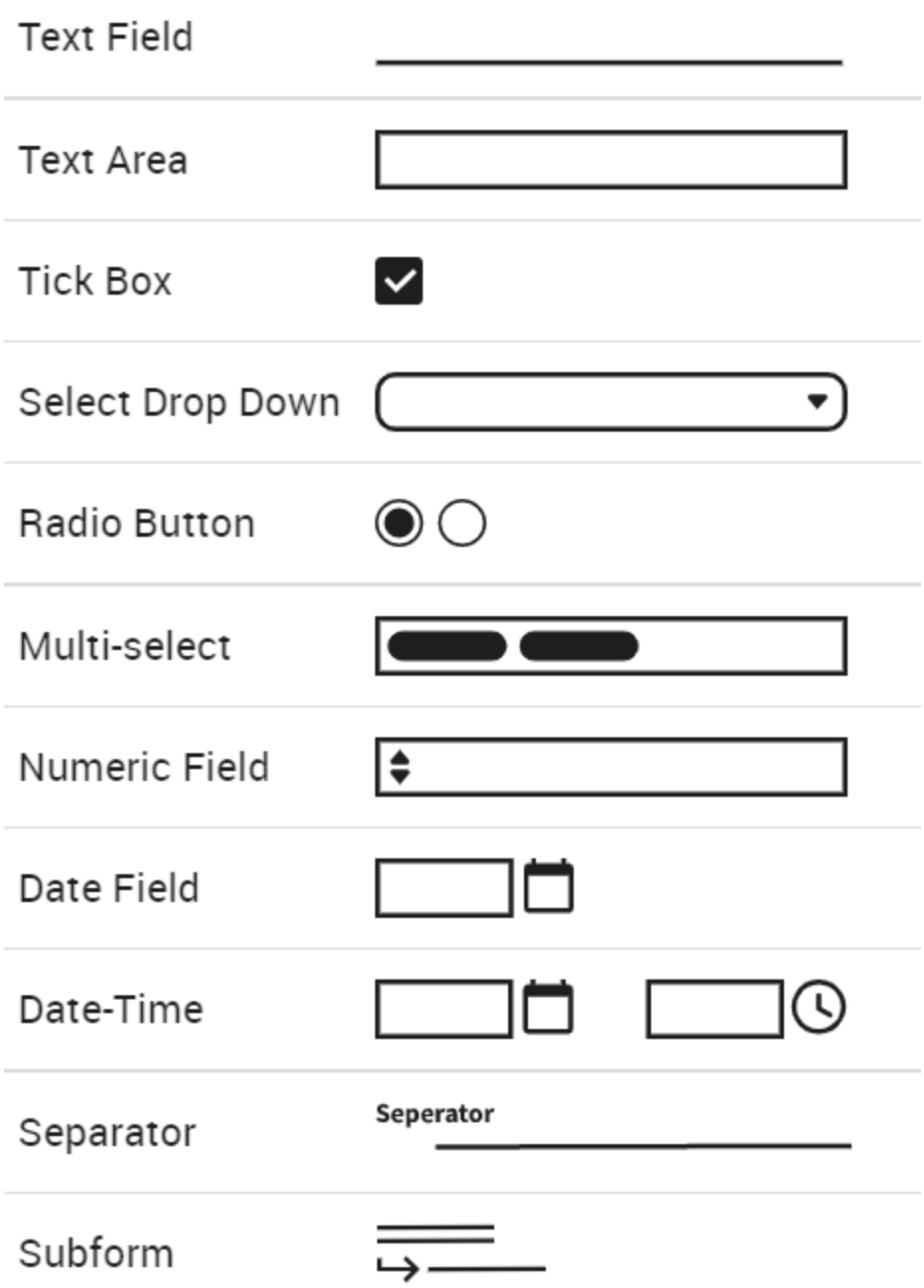
Create New Field

If you select the "Create New Field" option, you will be prompted to select a field type. Please be careful selecting the field type: *once you have selected a field type and saved the field, you will not be able to change the field type.*

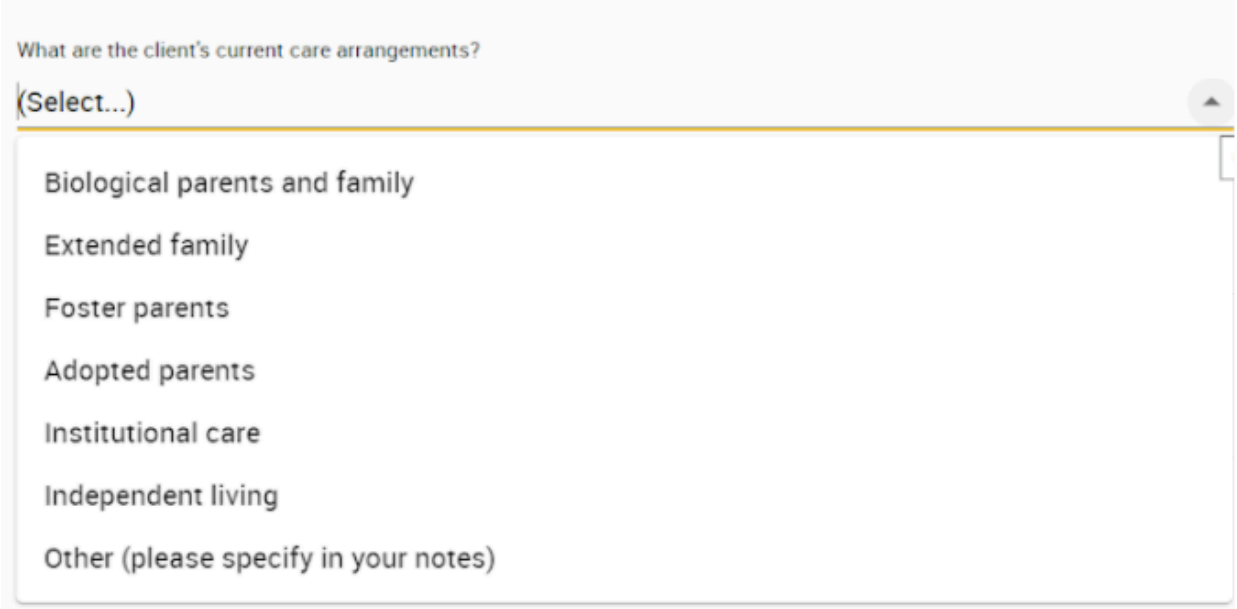


A brief description of each field type and any additional information to build the field is detailed below:

- **Text Field -** A Text Field is used for brief pieces of text. Unlike a Text Area, it will not expand to fit the text entered. Text will not be truncated but it is not easy to view.
- **Text Area -** Unlike a Text Field, a Text Area will expand to fit the text entered.
- **Tick Box -** A tick box is a checkbox with one selection as shown below:

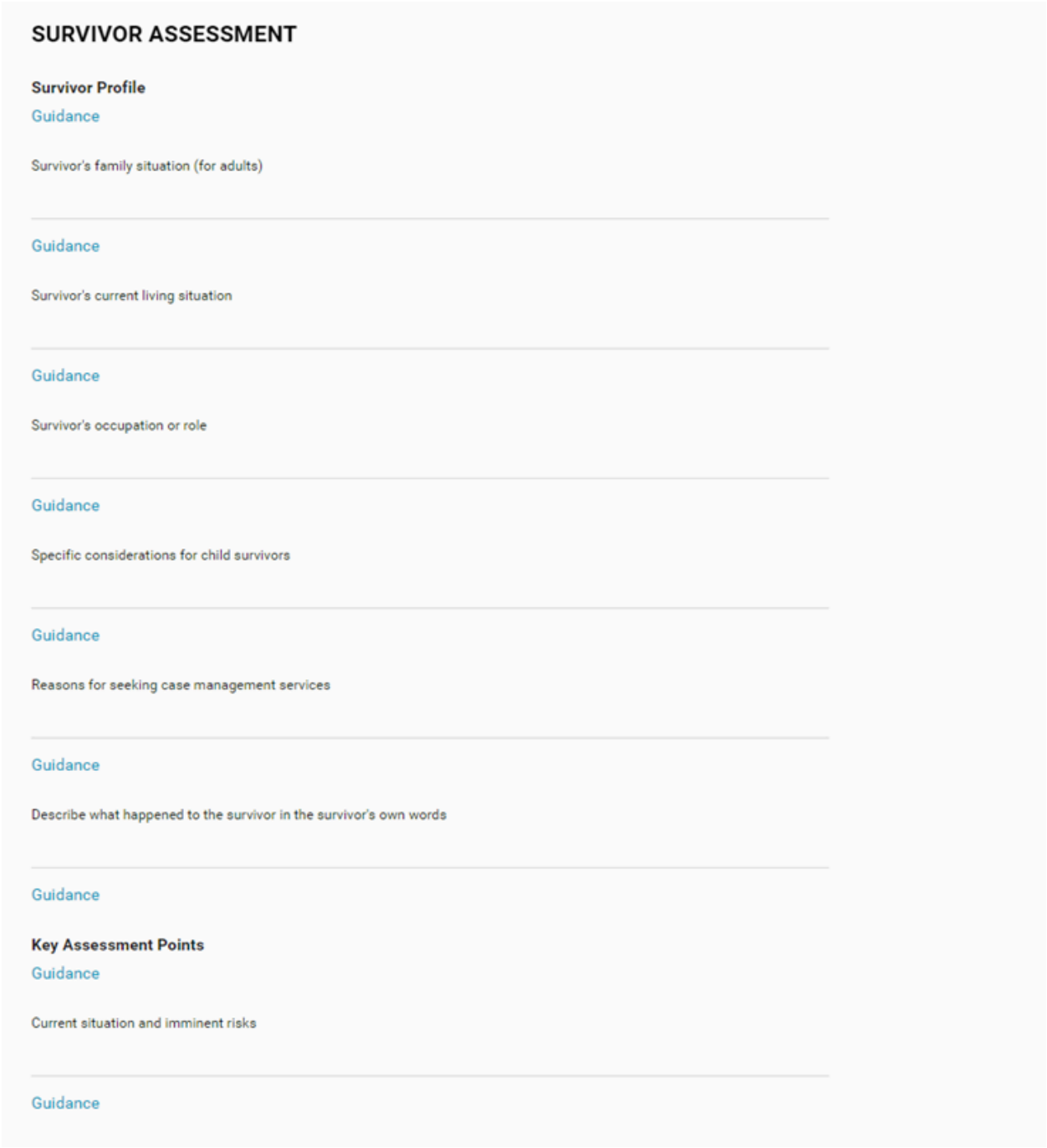


- **Select Drop Down** - A select drop down field allows the user to pick a value or values from a defined list of options as shown below:



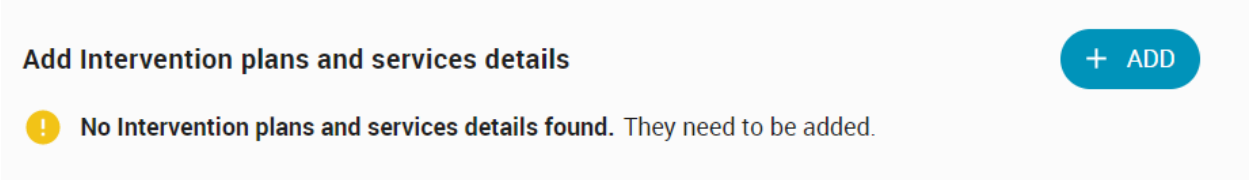
- **Radio Button -** This is similar to a Select Drop Down, since users can only select one option at a time. Note that, once a user selects an option, they cannot go back to having no options selected. This field type is typically used for Yes / No questions.
- **Multi-Select -** This is similar to a Select Drop Down, except that a user may select as many options as they like.
- **Date Field -** The date field type will automatically validate that what the user enters is a valid date field. The standard date format for Primero is dd-mmm-yyyy.
- **Date-Time -** This is similar to a Date Field, except that users can specify a time of day, in addition to a date.
- **Separator -** This is a header which separates one section of a form from another. For instance in CPIMS+, if the Child's Details form contains a number of fields about contact information for a child (e.g. "Location," "Address," "Phone Number"), you may add a Separator above these fields with the label, "Contact Information for the Child."

See example below from GBVIMS+: the Survivor Assessment form contains a number of fields about a survivor (e.g. "Survivor's family situation," "Survivor's current living situation," "Survivor's occupation or role"). There is a Separator above these fields with the label, "Survivor Profile" to distinguish these points from the "Key Assessment Points" below."

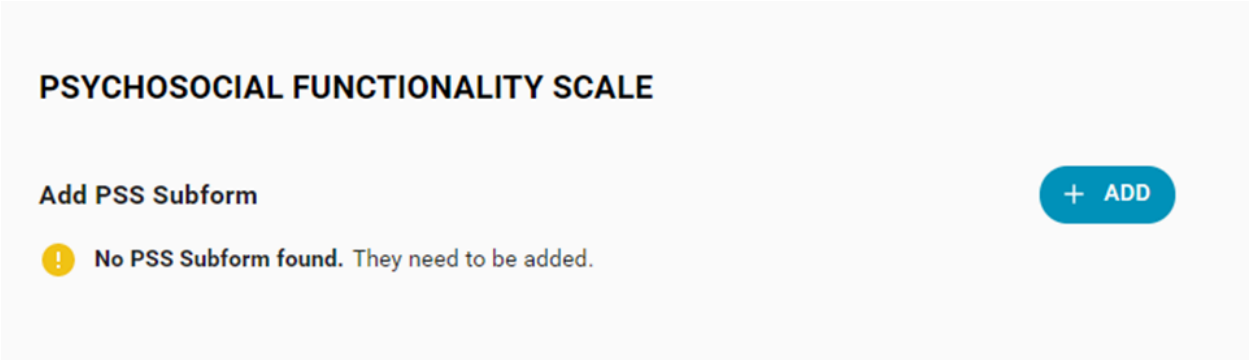


- **Subform -** The Subform is a section of a form where a user can collect the same set of data for multiple occurrences within the same Case, Incident or Tracing Request. For example, to collect information on a client's household member, a user may enter the "Age" and "Sex" for multiple people. For this reason, these fields appear in the "Household Members" Subform, where the user adds an entry for each household member. See example below for PCMIMS+:

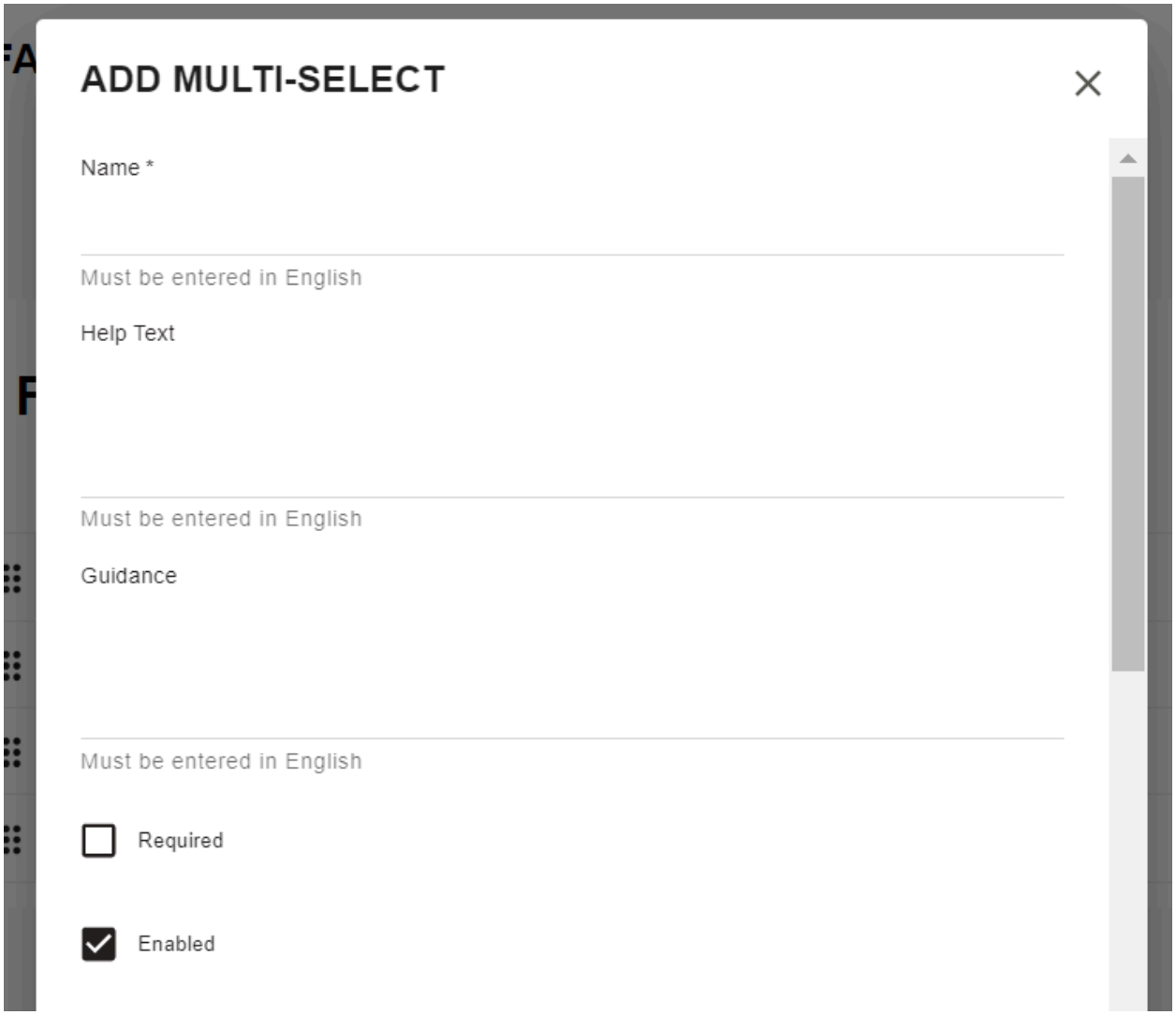
- See example below for CPIMS+:



In GBVIMS+, a case worker can complete the Psychosocial Functionality Scale with a survivor multiple times throughout the case management process. For this reason, this questionnaire appears in the “PSS” Subform, where the user adds an entry for each survey completed by the survivor. See example below:



Once a type of field is selected, the fields required to create that type of field will appear.



Below are the attributes you will need to specify for a field, though you will only need to specify some of these, depending on which field type you selected.

General Field Attributes

- **Display Name** - This is the field label that will display on the form
- **Help Text** - The help text will appear below the field and only in Edit mode. The help text is not visible when you are only viewing the record. This allows you to provide some guiding language to give the user a frame of reference for the proper answer or how to come to a conclusion based on information provided.
- **Guidance -** Similar to Help Text, Guidance is text you display to users to give guidance on how to fill out the field. Generally, Guidance is for guiding text which is too long to put into Help Text. Users view Guidance by clicking the “Guidance”

link below a field, at which point a small box appears containing the configured Guidance text.

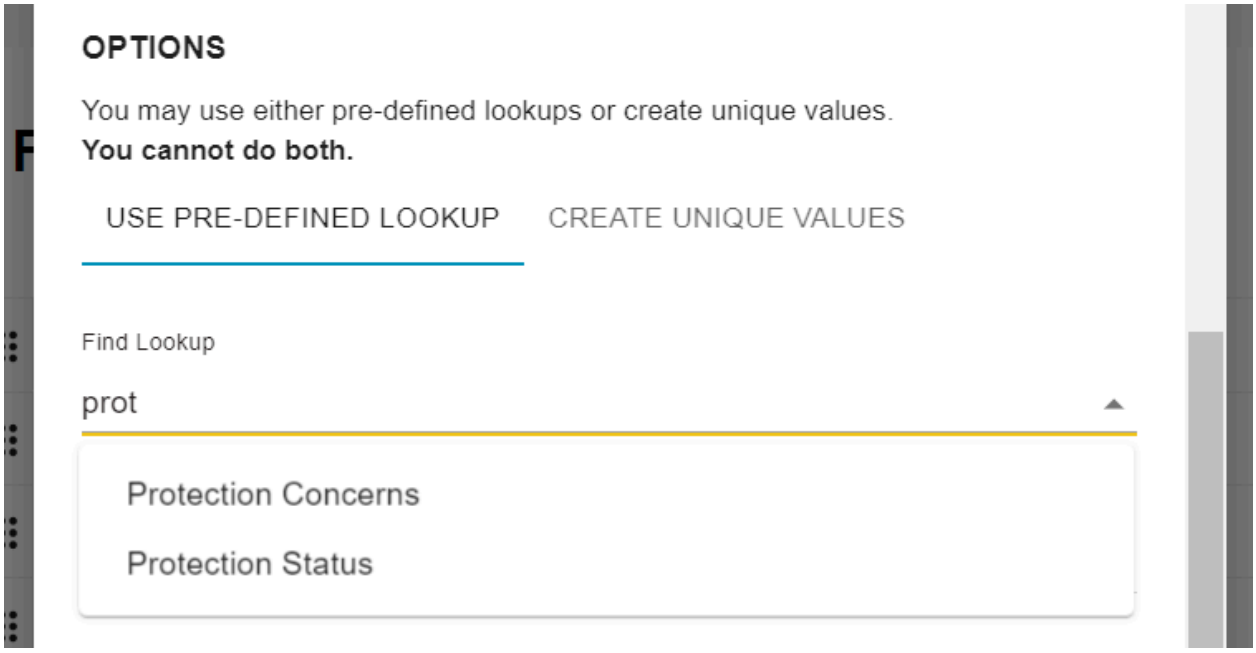
- **Required -** If a field has this attribute checked, users will not be able to save a record without filling out the field. *Note that if a field inside a subform is required, users will only be required to fill out the field if they have already added an entry into that subform.*
- **Enabled -** Set to checked by default, this attribute determines whether users can update information in a field, or whether they can only view that information. If this is checked, users can update information in the field; if not checked, they cannot update the field's information.

Specifying Field Options

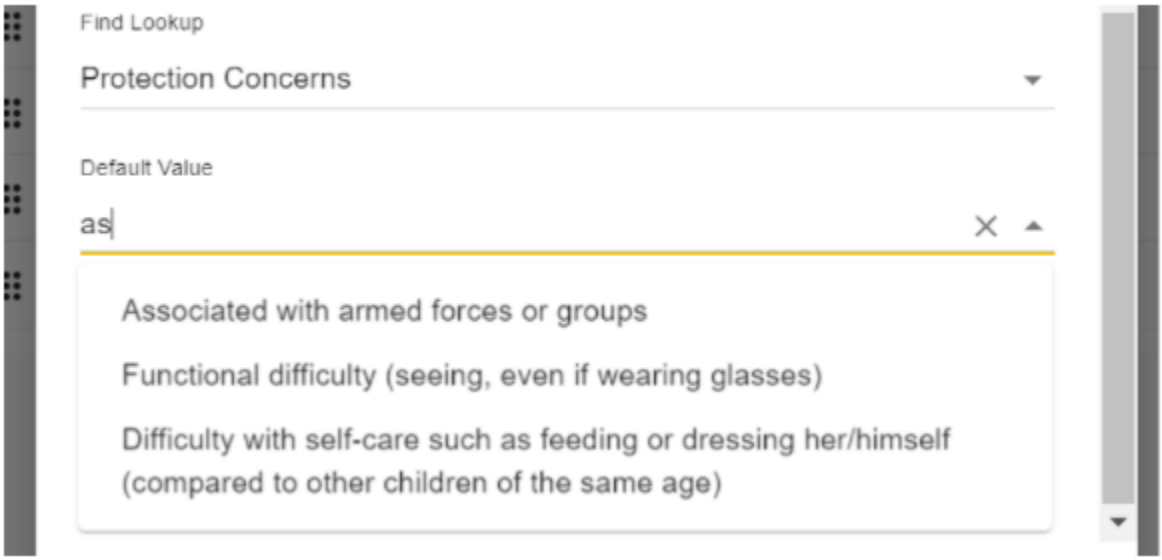
For Select Drop Downs, Multi-Selects, and Radio Buttons, there are two ways to specify options:

- **Use Pre-Defined Lookup -** A Lookup a list of options that can be reused across multiple fields. For example, the Country Lookup (containing the names of all the world's countries) is used by fields like "Nationality" and "Country of Origin." Using a lookup helps you avoid specifying the same options multiple times when configuring forms. *It is highly recommended to use Lookups whenever possible.* For more information on Lookups, as well as how to create and update them, see the **Lookup Values Management** section of this guide.
- **Create Unique Values -** If your field will need options that will not be used by any other fields, you can specify unique option values.

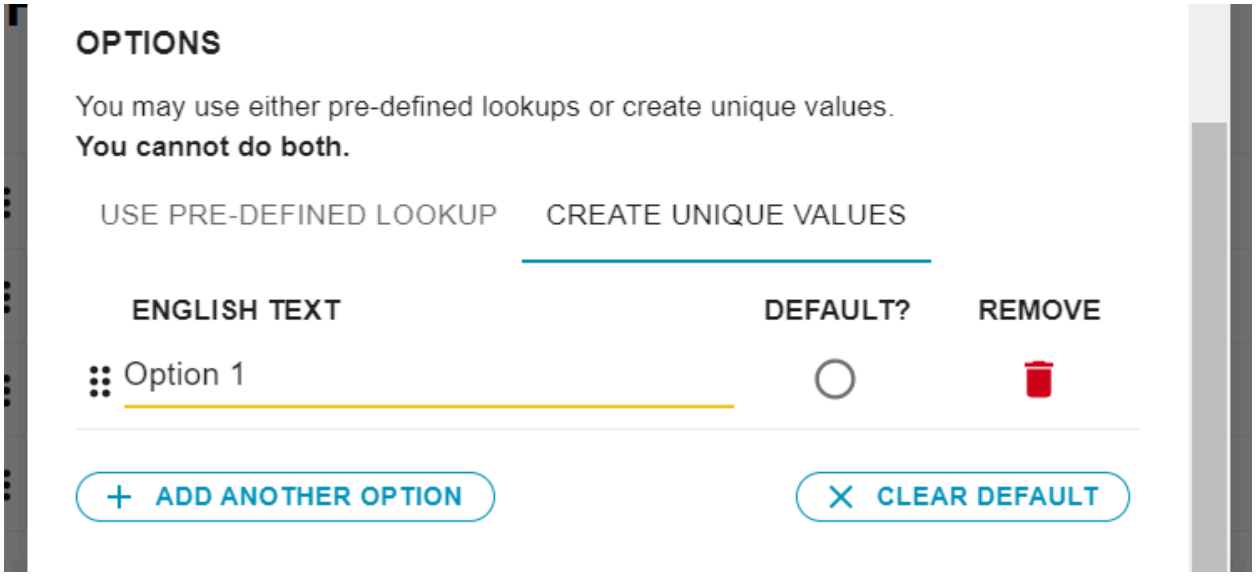
To specify a Lookup to use for your field's options, click the "Use Pre-Defined Lookup" tab in the "Options" section of the form. Then begin typing in the "Find Lookup" field to search for the Lookup you want.



Once you have selected a Lookup, you can also choose one of the Lookup's options to be selected by default when a user creates a new record.



To specify unique options, click the "Create Unique Values" tab. Add as many options as you want. Use the radio buttons in the "Default" column to select which option should be populated by default when a user creates a new record. You can drag-and-drop options to rearrange them.

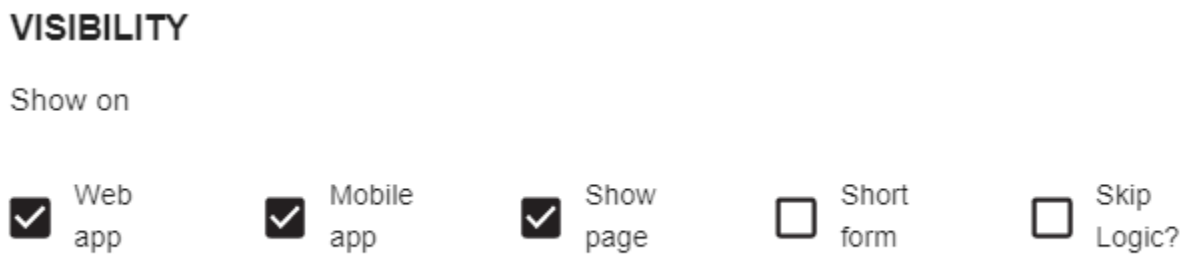


NOTE: Please be careful when selecting options. Once you have saved a field, you will not be able to ...

- Change the Lookup used for its options
- Switch from using a Lookup to using unique option values.
- Delete options from Unique Values.

Setting Visibility

At the bottom of the Add Field pop-up, you will see four tick boxes which control where the field appears.



- **Web app** - This controls whether the field appears for users when they are viewing, editing, or creating a record.
- **Mobile app** - NOTE: This attribute no longer controls anything. It may be removed in the future.

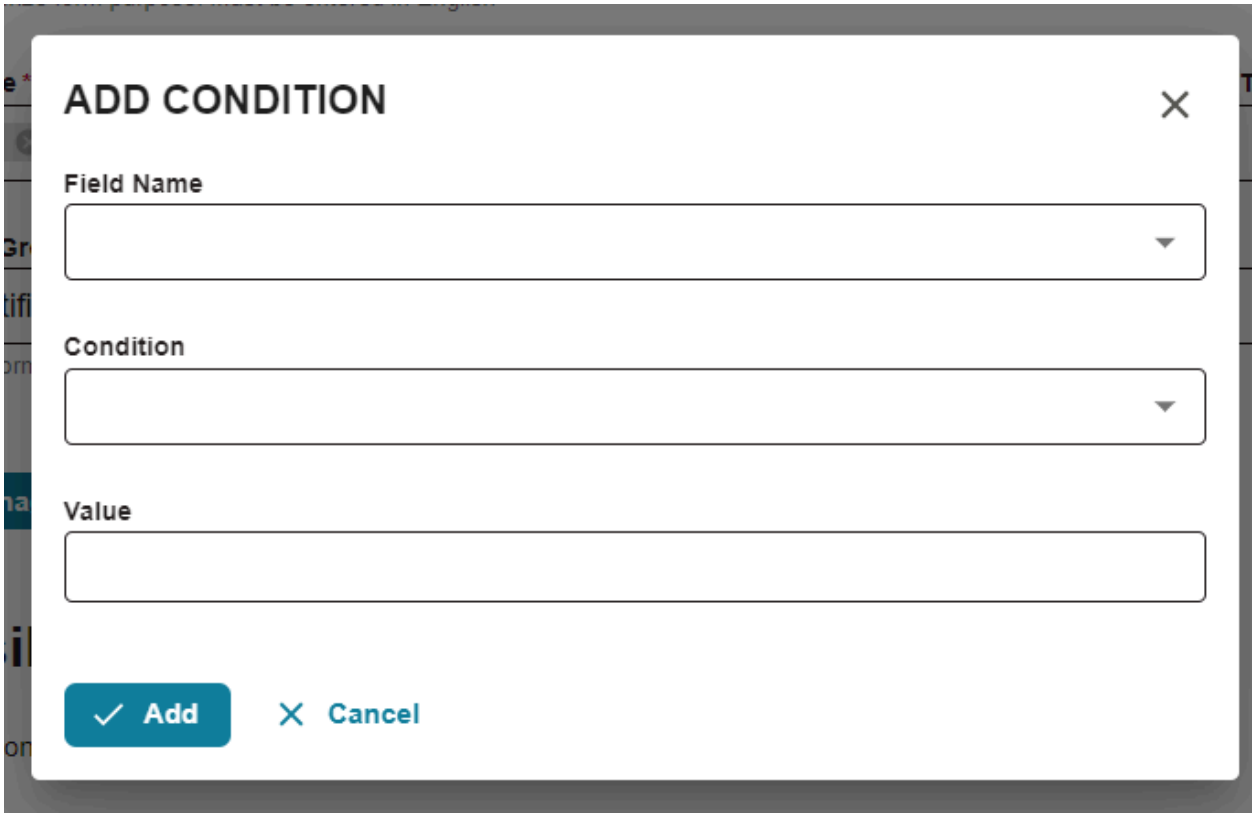
- **Show page** - Checking this box allows the user to see the field when they are viewing a record. If the box is unchecked, the field will only be visible when they are creating or editing a record.
- **Short form** - If this box is checked, the field will appear to users who are previewing records they cannot access.
    - Note that this attribute will not appear for fields which are located within subforms.
    - Note: if you would like to “hide” the photo from appearing in the preview modal when a case worker searches for a case, preview modal, then edit the "Photos and Audio" form, click into the "Photos" field and, under "Visibility," uncheck "Short form".
- **Skip logic?** - Checking this box allows the user to add conditions on the field to enable skip logic. Go to “Specialized Attributes” to read more about skip logic.

Specialized Attributes

Some form attributes only appear for specific types of fields:

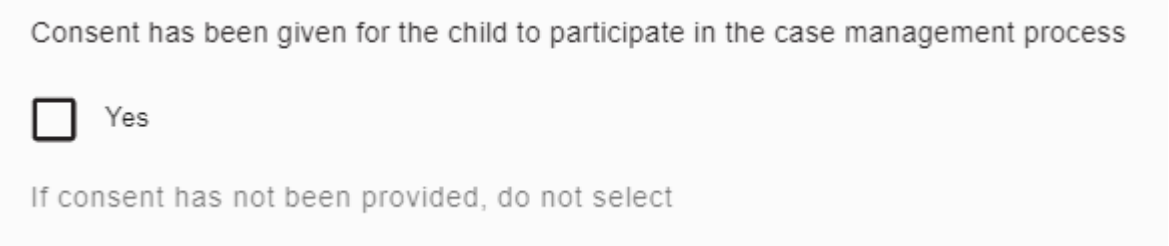
- **Skip Logic -** Conditions can be made on specific forms and fields where you can “skip” specific forms or fields based on a response on another question. In order to enable skip logic, you will select the “Skip Logic?” tick box under “Visibility” on the form itself or within a field in a specific form. Once ticked, you will be able select the “Add Condition” which will allow you to select a specific response which would ensure a question or form is skipped. You can set multiple visibility conditions for a form and combine them, saying either that all conditions need to be true or only one needs to be true. Here is a short video providing guidance on

how to configure skip logic.



Note: Let's say you create a skip logic where B will only show if you select A, and C will only show if you select B. If you add a value for A, and then later hide A, it does not hide C. This is by design, since clearing out the values for fields once they were hidden could cause confusion with users.

- **Tick Box**
  - **Tick Box Label -** This is the label which appears to the right of a tick box. If left blank, users will see the word "Yes" to the right of the box, as seen below.

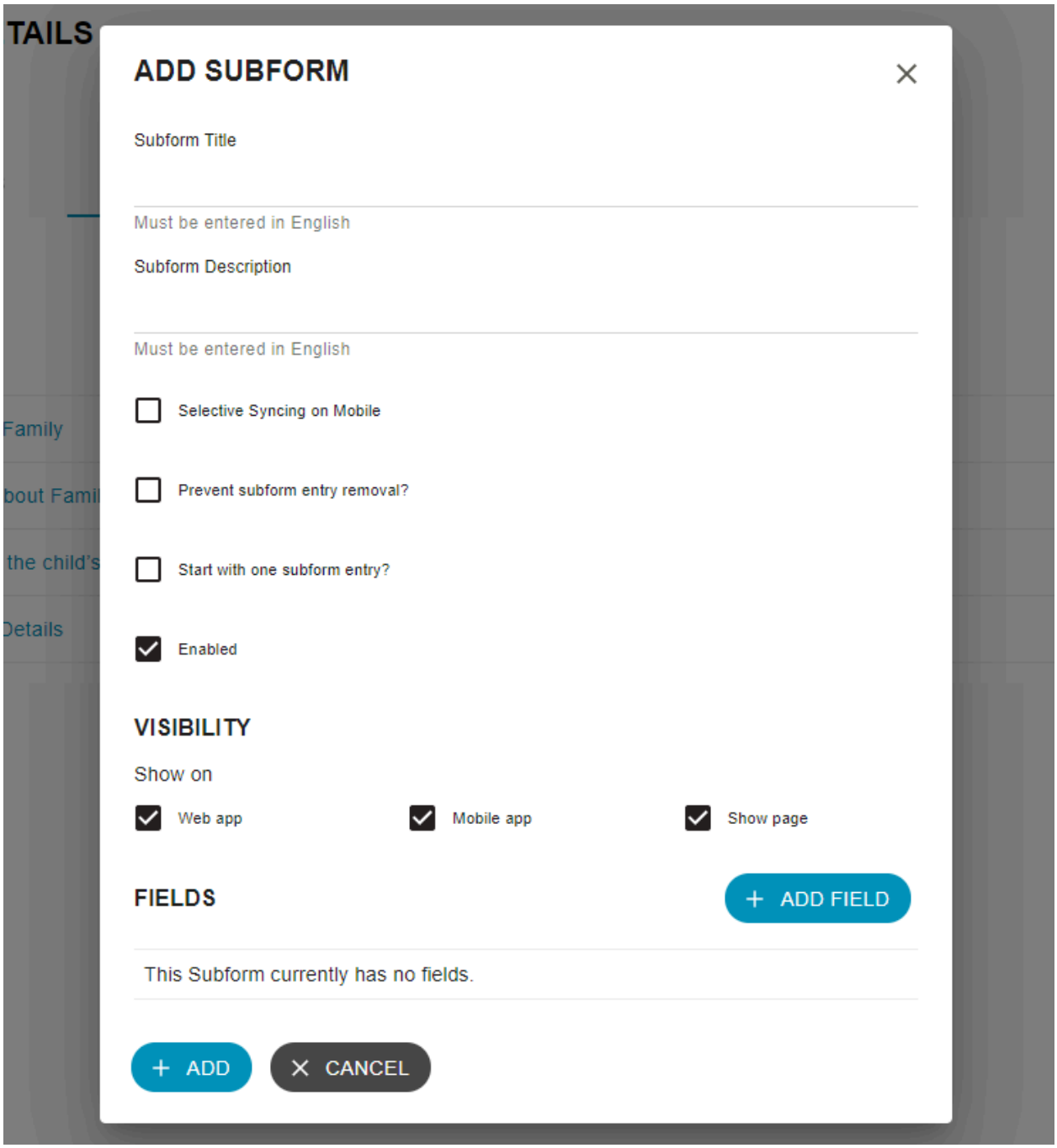


- **Date Field** and **Date-Time**
  - **Cannot be in future -** Checking this box will prevent users from entering dates or times in the future for this field.

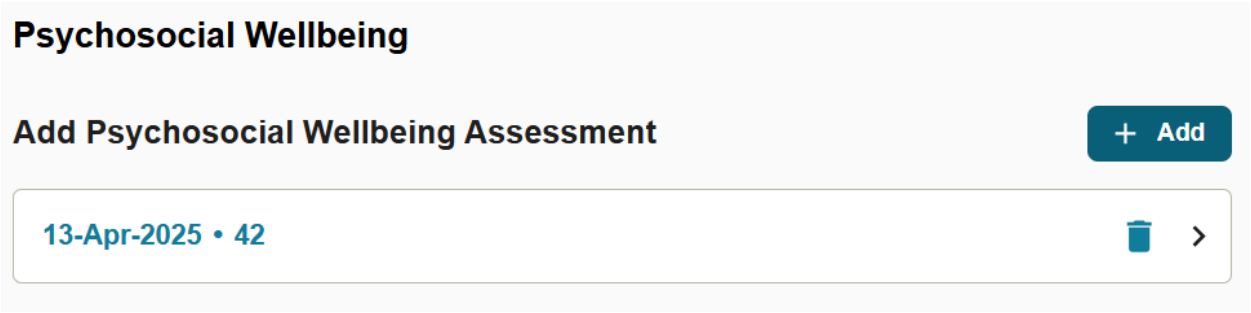
- **Defaults to current date? -** If this box is checked, users creating a new record will see this field with the current date automatically filled.
  For **Date-Time** fields, this attribute appears as "**Defaults to current date and time**," since users creating new records will see the field automatically filled out with the current date and time.

Adding a Subform

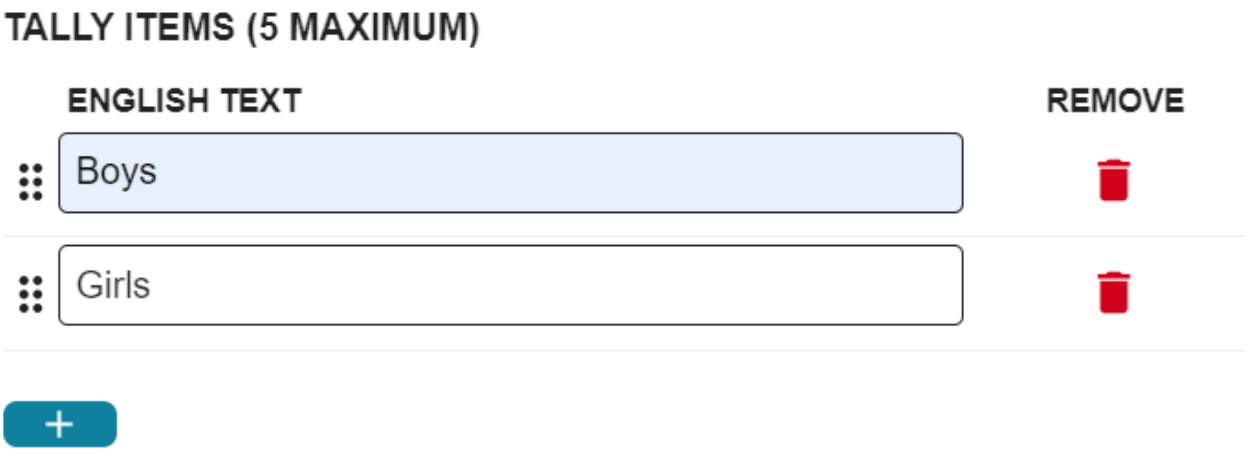
If you select "Subform" as the field type, you will see specialized attributes for Subforms.



- **Subform Title -** This will appear at the top of the modal for adding subforms, and as part of the header above your subform. See example below.



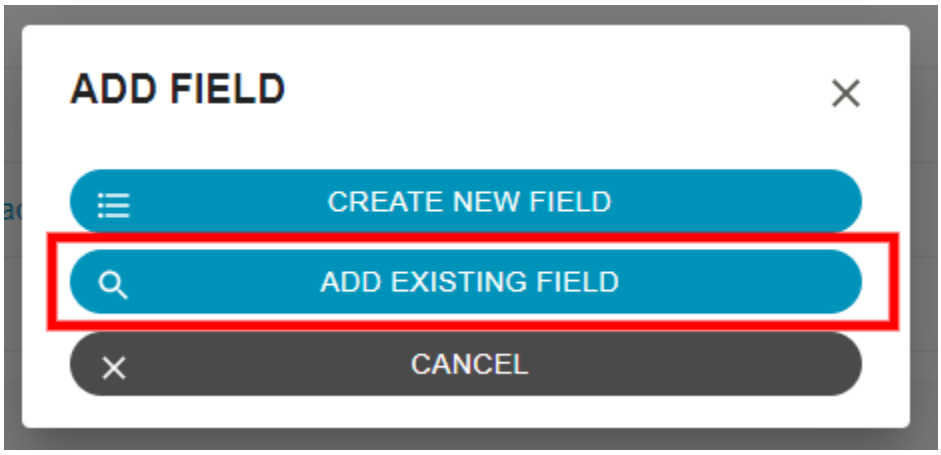
- **Subform Description -** This description is only visible to administrators.
- **Selective Syncing on Mobile -** NOTE: This attribute no longer controls any functionality. It may be removed in the future.
- **Prevent subform entry removal? -** Checking this box will prevent users from removing a subform entry once they have added it. This is typically used for subforms which are critical to Primero functionality, such as the Services subform.
- **Start with one subform entry? -** If this box is checked, when users create a new record, they will see one blank entry automatically added for this subform. Note that selecting this setting while including required fields in your subform can help ensure users fill out at least one subform entry on record creation.
- **Tally Field**
  - **Tally Items -** These are the items which users will tally (up to a maximum of 5 items) as seen below.



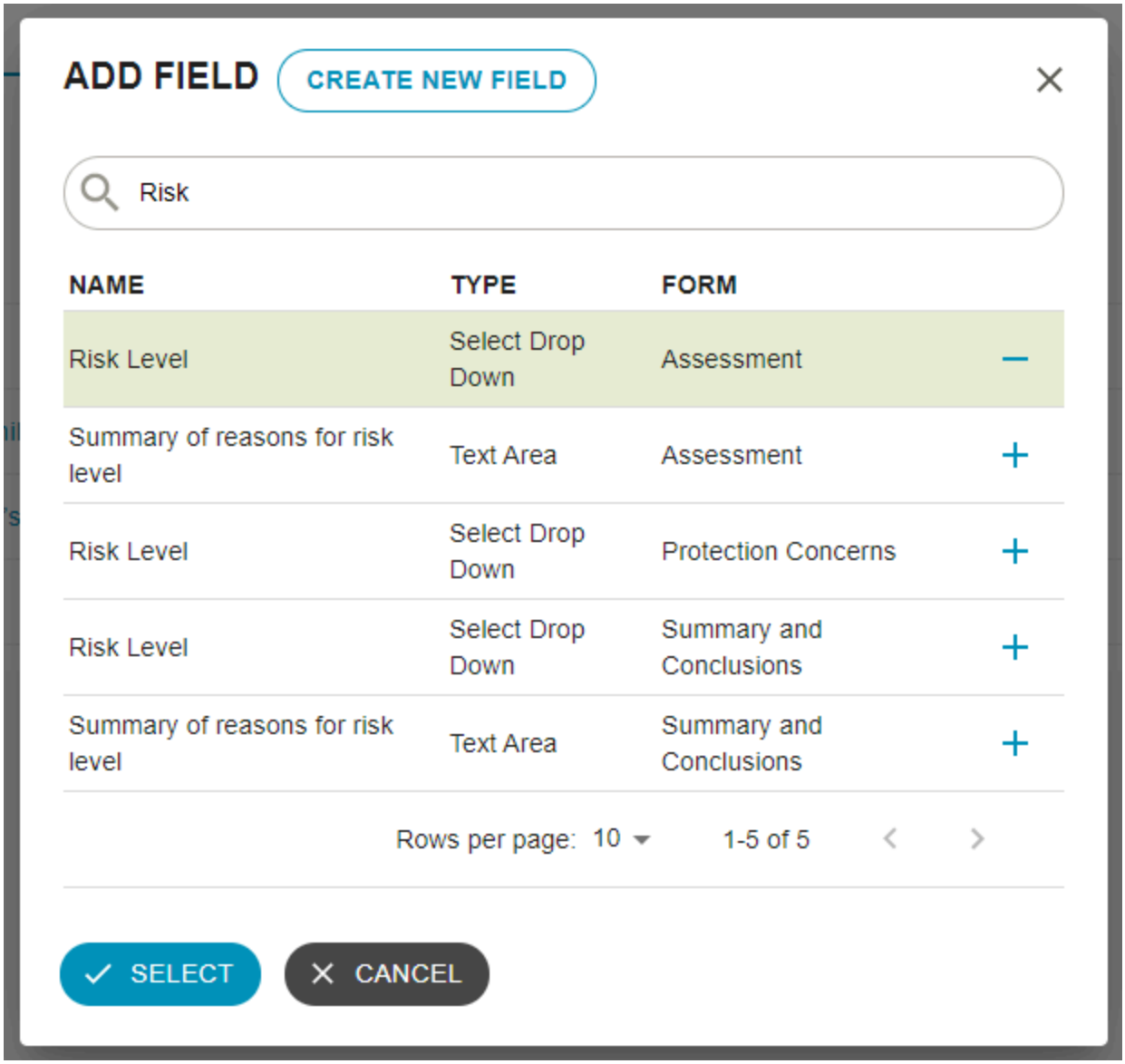
Once Boys and Girls are added, the tally looks like this on the form:

Add Existing Field

To copy a field to your form which has already been created on another form, click the “Add Existing Field” button after clicking the Add field button.



In the search box, type to find a field. Click the ‘+’ next to the field you want to add.



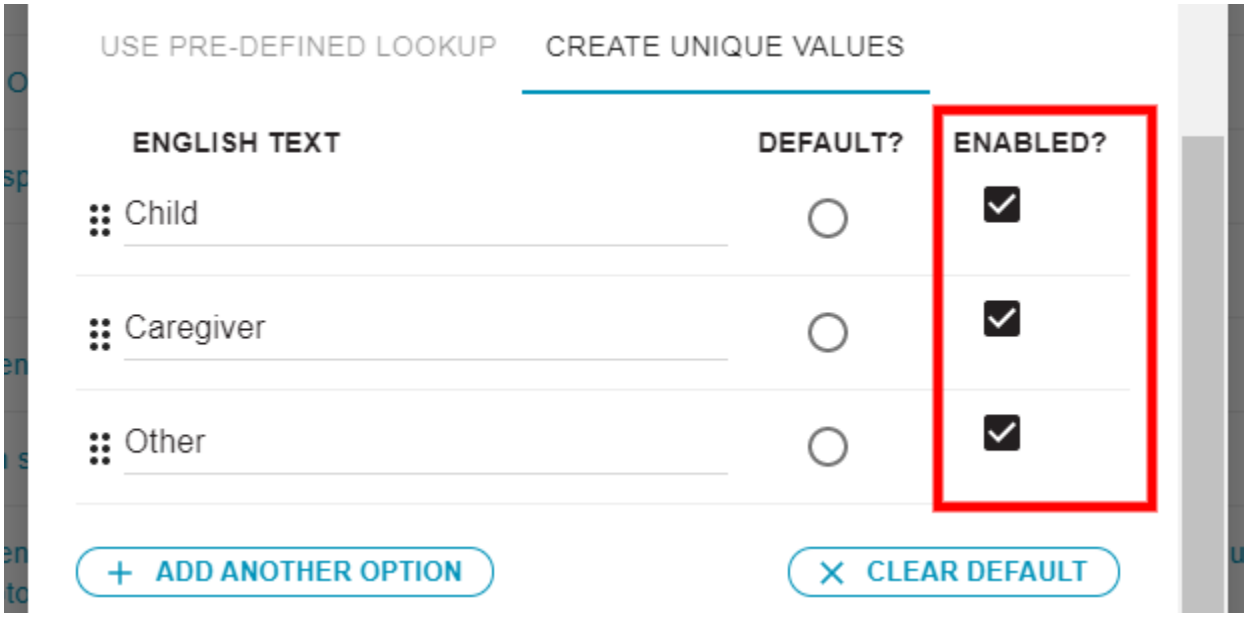
Once you have selected the field, search for other fields to add. If you want to deselect a field, click the '-' which appears where the '+' was previously. Click the "Select" button when you are done.

Updating Fields

To edit a field, go to the Fields tab of the form editor, then click the field you want to edit. Editing a field is very similar to adding a field, with the following exceptions:

- You cannot change a field from one type to another. If you would like to change a field's type, you must create a new field with the desired type, then hide the field you are replacing.

- You will not be able to change all of your field's option configuration. Specifically, you will not be able to ...
  - Change the Lookup used for its options
  - Switch from using a Lookup to using unique option values.
  - Delete options from Unique Values. Instead, if you no longer want one of your unique values to appear, you can deselect the tick box next to the option in the "**Enabled**" column of the option list. This will prevent users from selecting this option in the future.



***Note**: You cannot delete fields in Primero. If you created a field by mistake or do not want it to appear in the forms anymore, you can hide it using the "**Visibility**" tick boxes in the Edit Field modal.*

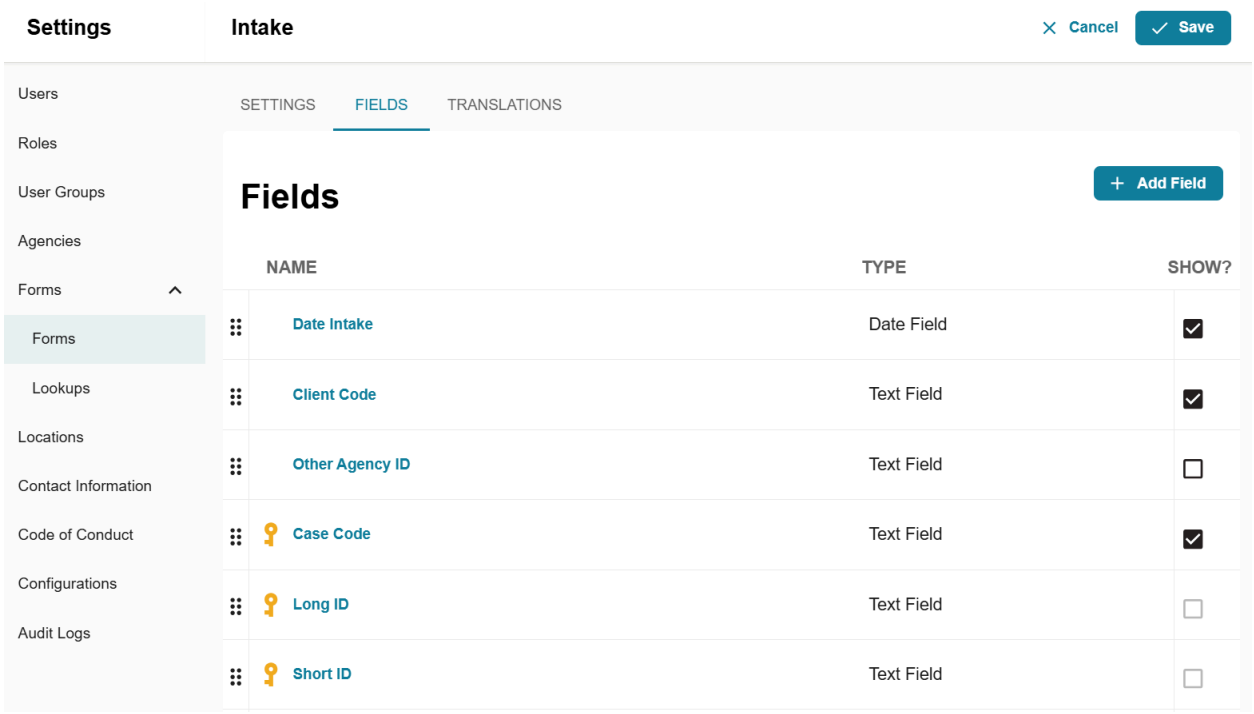
Editing an Existing Form

To edit an existing form, go to the Forms list and click the form you would like to edit. You will automatically arrive at the Edit Form page. Once you have made changes, **be sure to click the Save button.** If you do not click Save, your changes will be lost.

Editing a form is mostly similar to creating a form. Note that you cannot add fields or translations for your form until you have saved it.

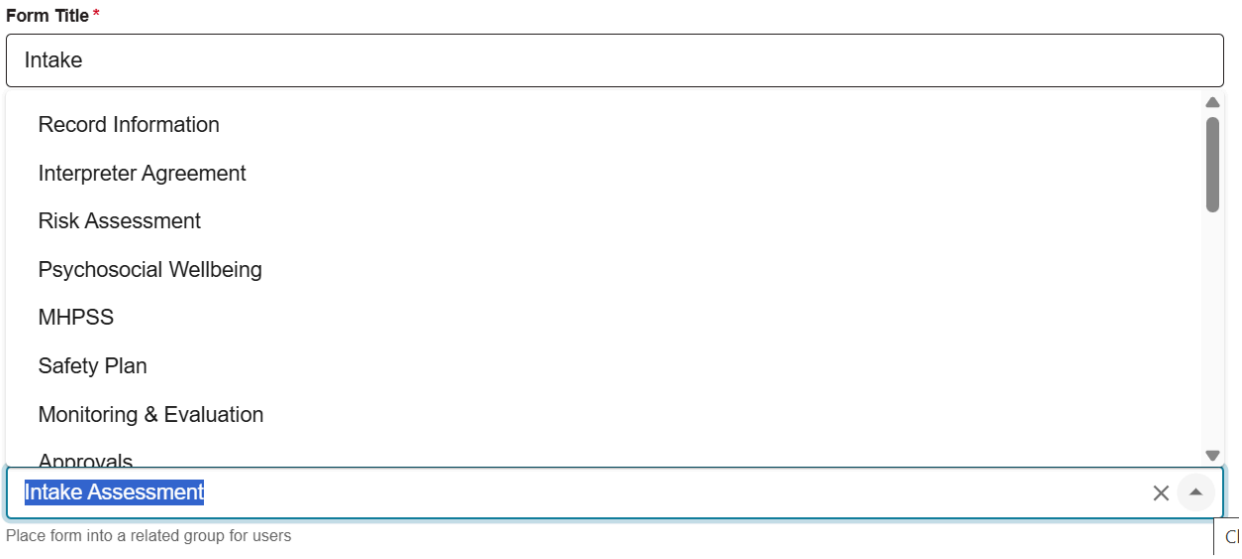
Change the Field Order within a Form

While editing a form, you can change the order of fields. Drag and drop fields using the "grip" at the left side of the fields table.



Change the Form Group

While creating or editing a form, you can change the form group by clicking into the Form Group field. Begin typing the name of the form group you want and then select one of the results that appears.

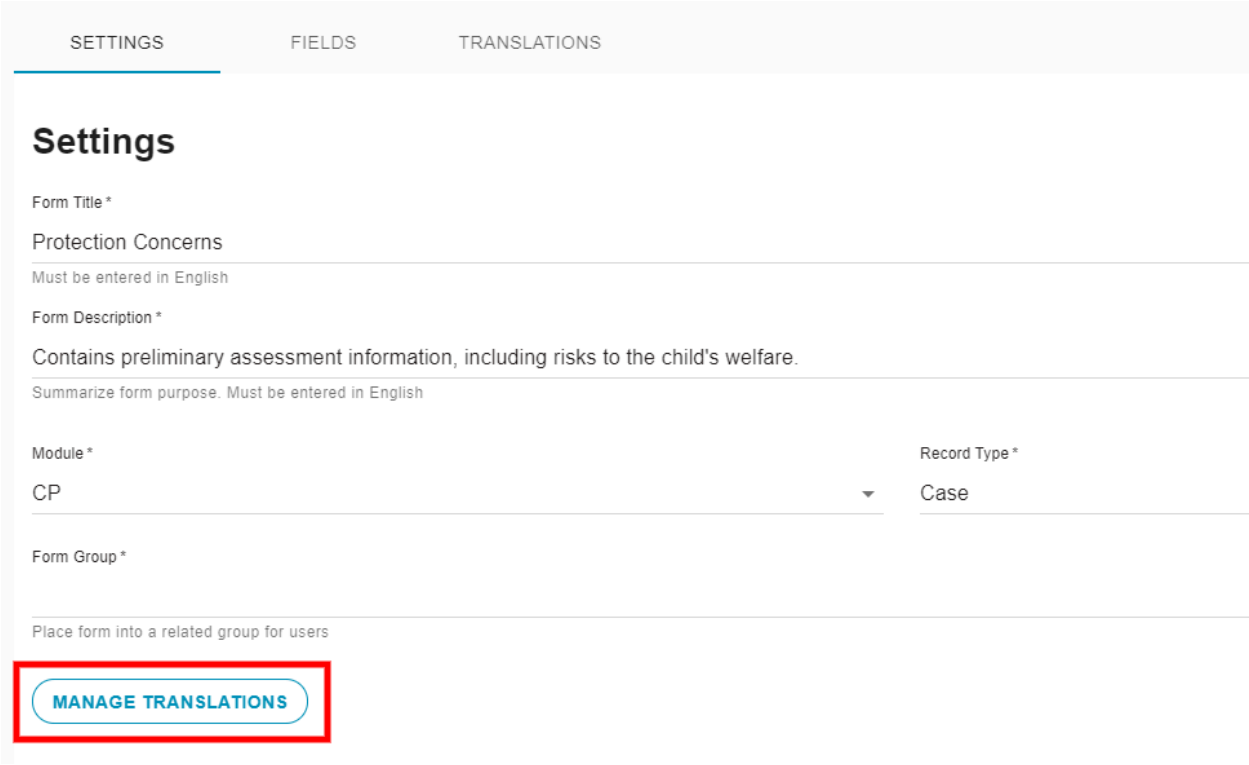


To add a new form group, type the name of the new form group in the field. Then click the “Add” option that appears. Once you save the Form, this new Form Group will be added.

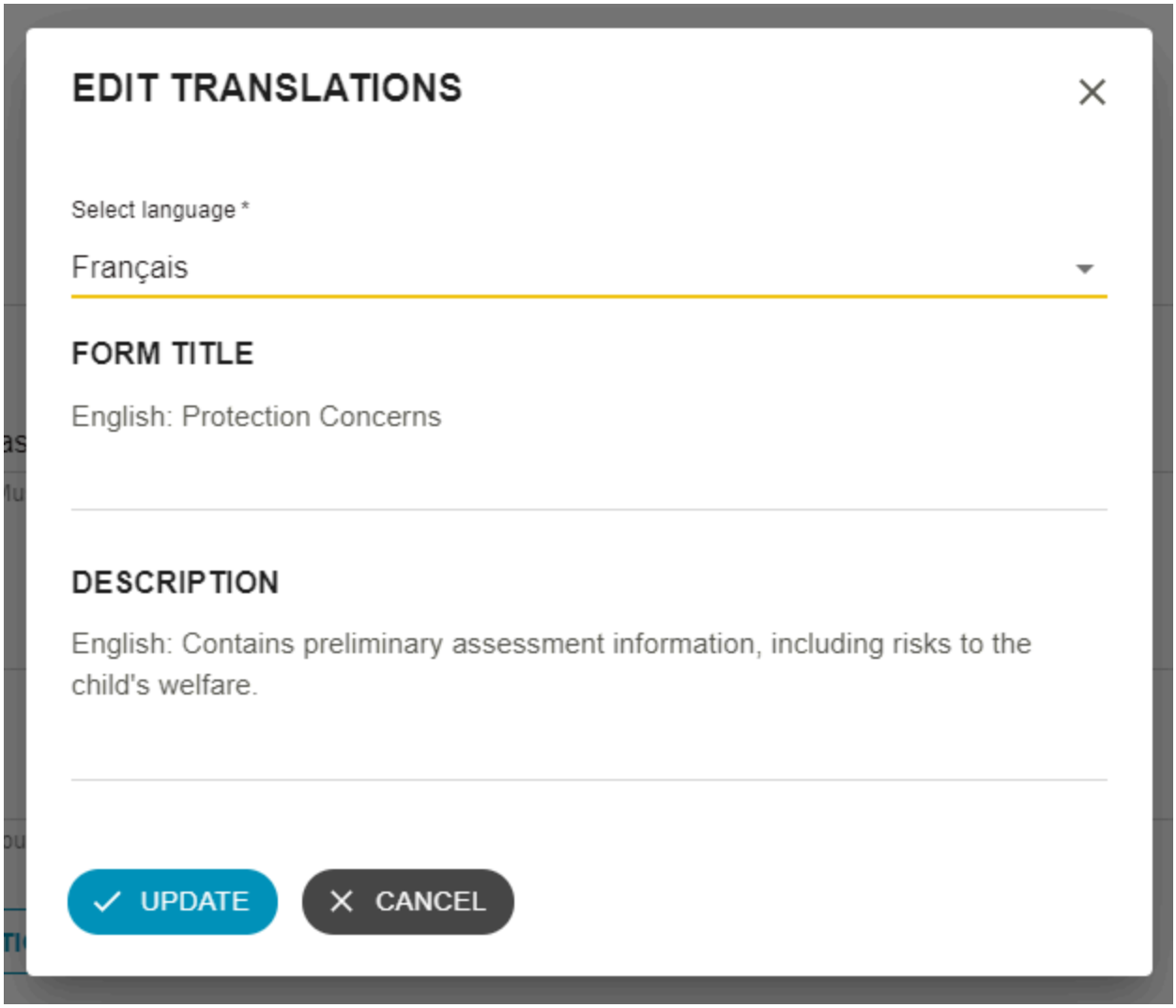
Providing Translations

NOTE: You cannot provide translations for a form until it has been saved. You must create and save a form with its English name before you can provide translations.

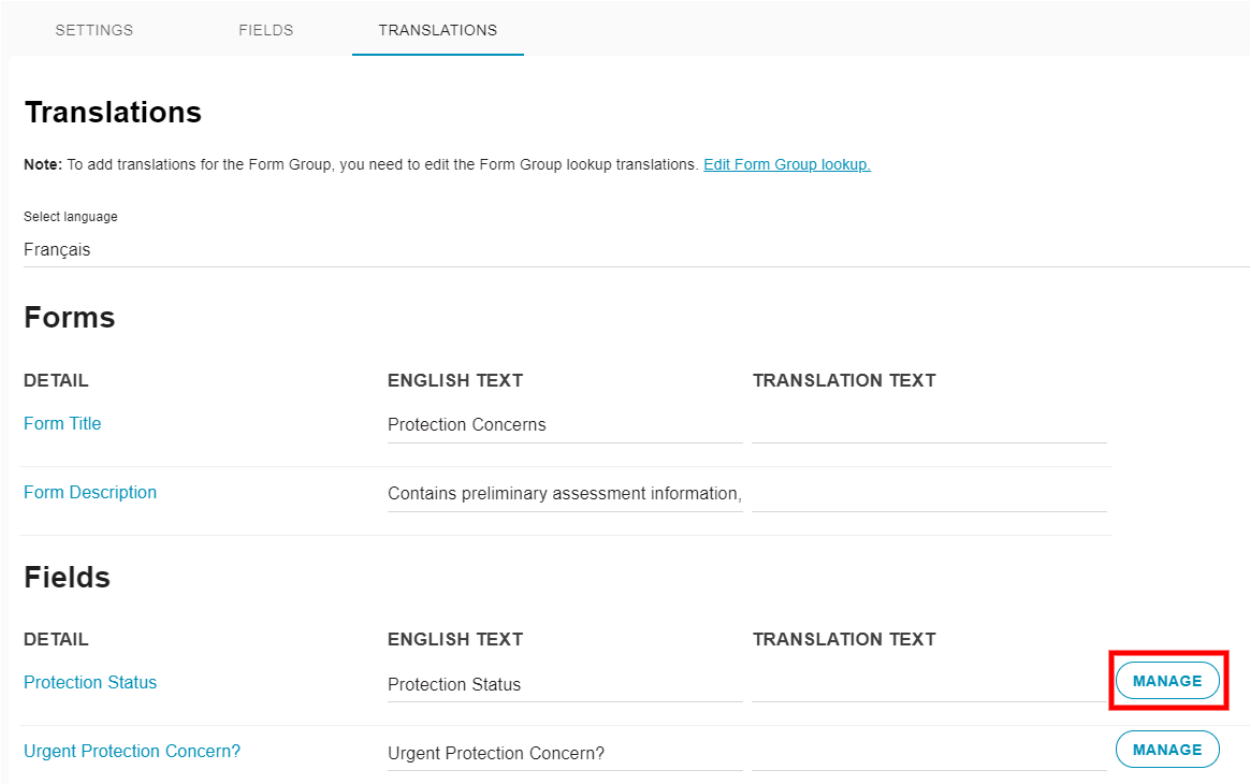
To provide translations for a Form's main attributes, click the **Manage Translations** button on the Settings tab.



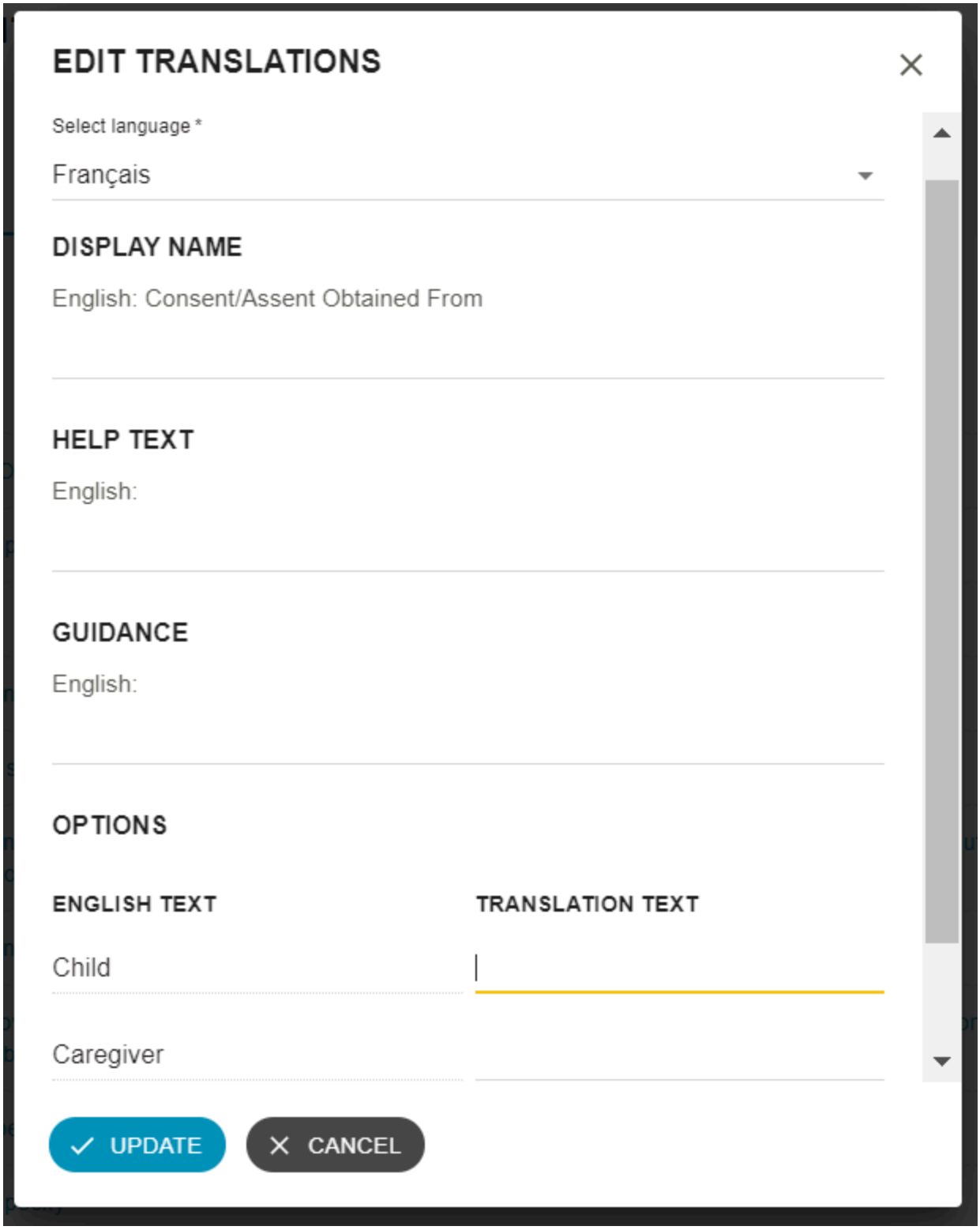
The Manage Translations modal will open. Select a language from the "Select language" dropdown, then enter your translations. Click the **Update** button when you are done.



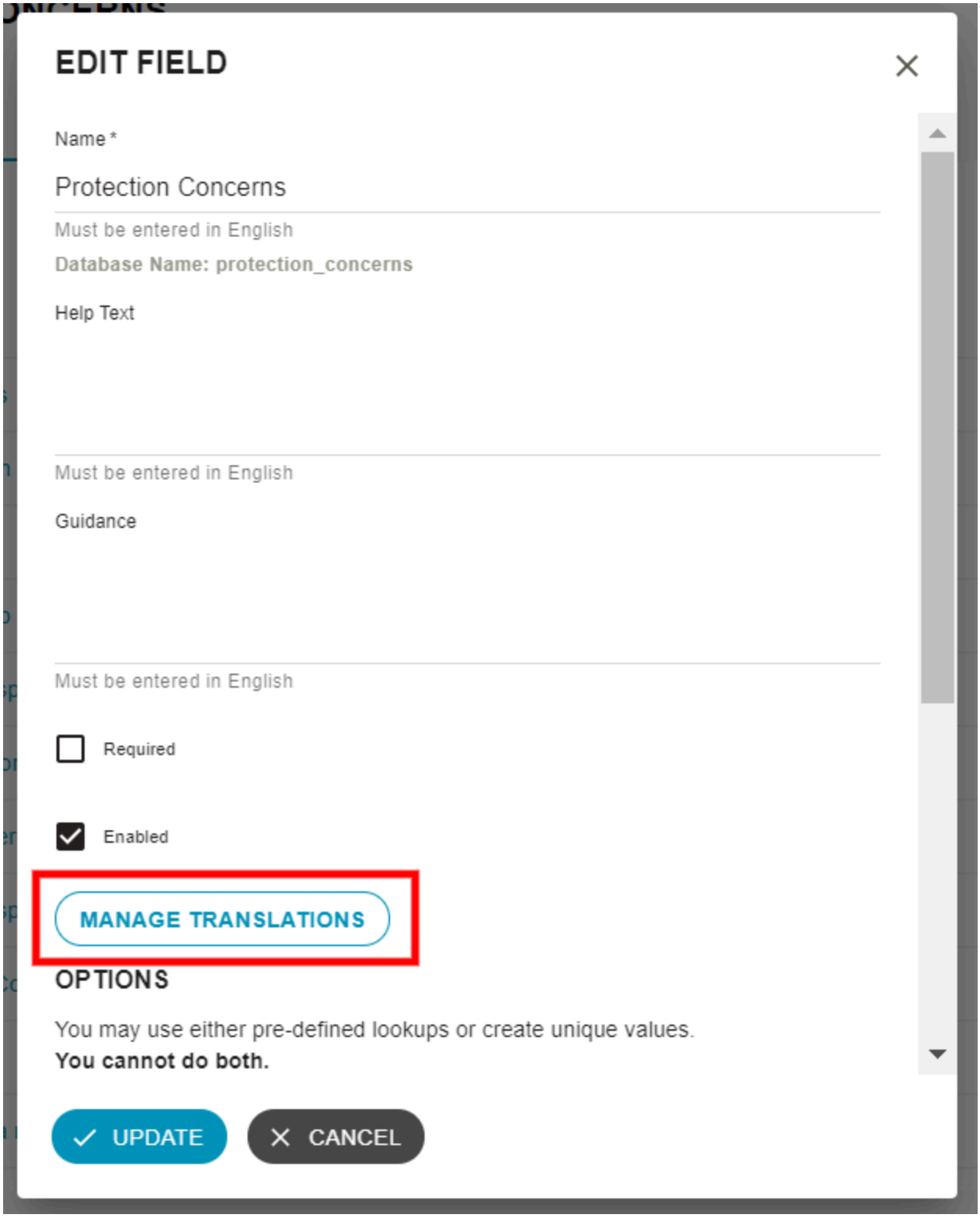
You can also provide translations by clicking on the **Translations** tab in the Form Editor. Here, you can provide translations for settings like the Form Title and Description, as well as for the display names of any fields. Be sure to select your translation language before entering translation text.



If you would like to provide more detailed translations for a field, click the **Manage** button next to that field. The Manage Translations modal will appear for that field. Select the language, provide translations, and click **Update** when done.



You can also provide translations for field attributes in the Edit Field modal. Go to the Fields tab of the Form Editor and click a Field to edit it. Then, inside the Edit Field modal, click the **Manage Translations** button.



The same Manage Translations modal will appear for the field. Select a language, enter translation text, then click **Update** when you are done.

Once again, please be sure to click the **Save** button at the top of the Form Editor page once you are done making any changes to Form or Field translations.

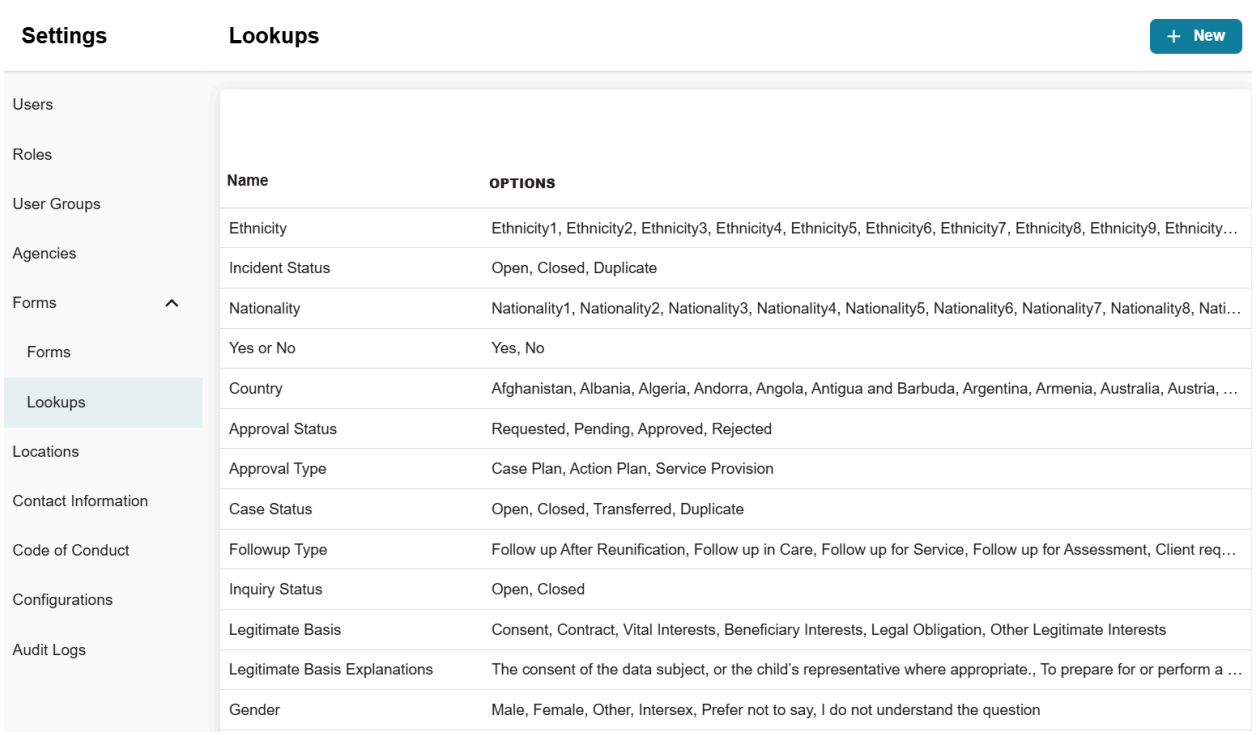
***Note**: While you can manage unique field options in the Manage Translations modal, you cannot use this interface for translating Lookup options. For information on how to translate Lookup options, please see the **Lookup Values Management** section of this guide.*

***Note:** if you are changing a translation for a field that is shared on multiple forms, please follow these steps:*

1. *Update the name translation in the original field*
2. *Remove the fields which shared the original field if there is no data to be preserved*
3. *Re-add the field to the other forms*

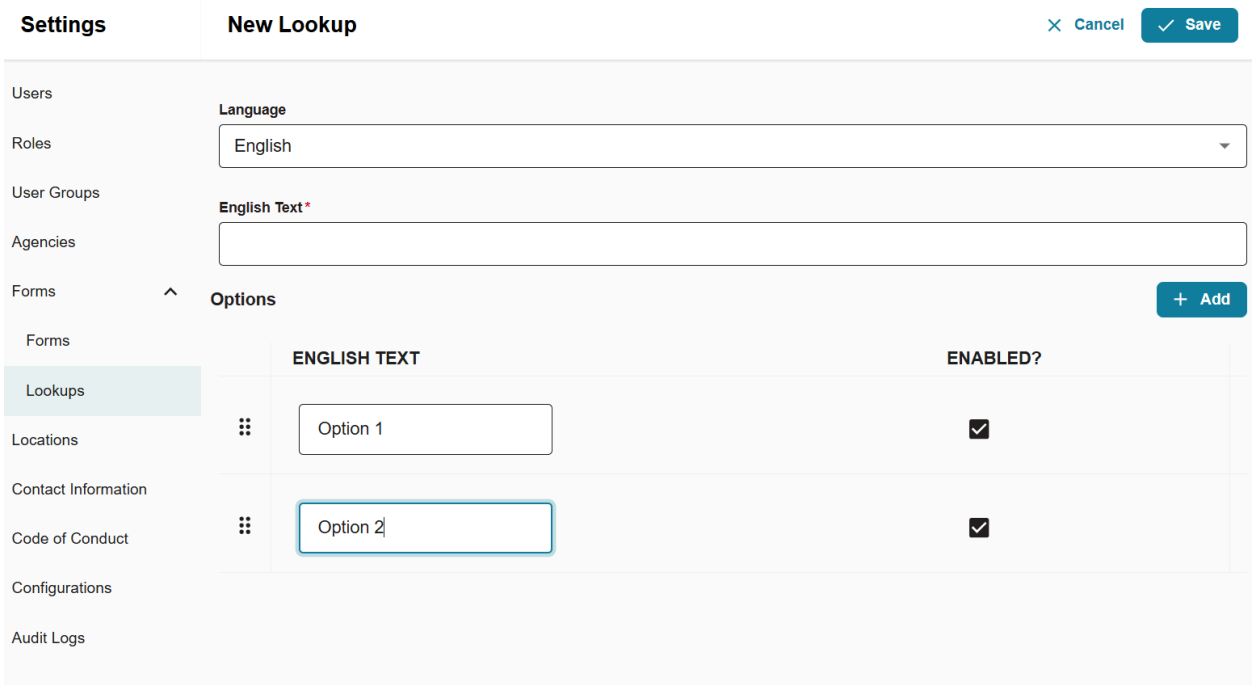
Lookup Values Management

“Lookup” is the term used for a set of values that might be used as the dropdown options for multiple fields. For example, the Country Lookup (containing the names of all the world’s countries) is used by fields like “Nationality” and “Country of Origin.” Using a lookup helps you avoid specifying the same options multiple times when configuring forms. To view all configured lookups, click the **Settings** link in the navigation menu. In the Settings navigation menu, open the “Forms” group, then click the **Lookups** link. You will then arrive at the Lookups list.

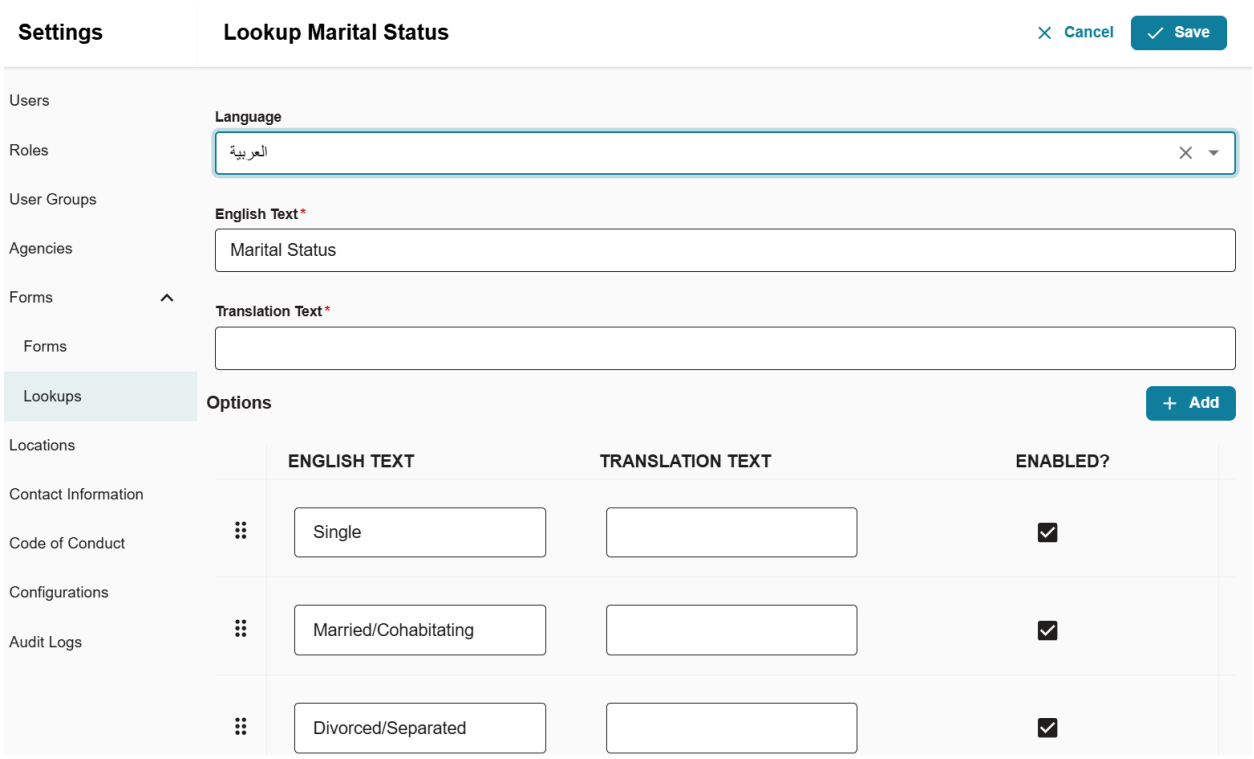


Creating a Lookup

To create a new lookup, click the New button at the top of the page.

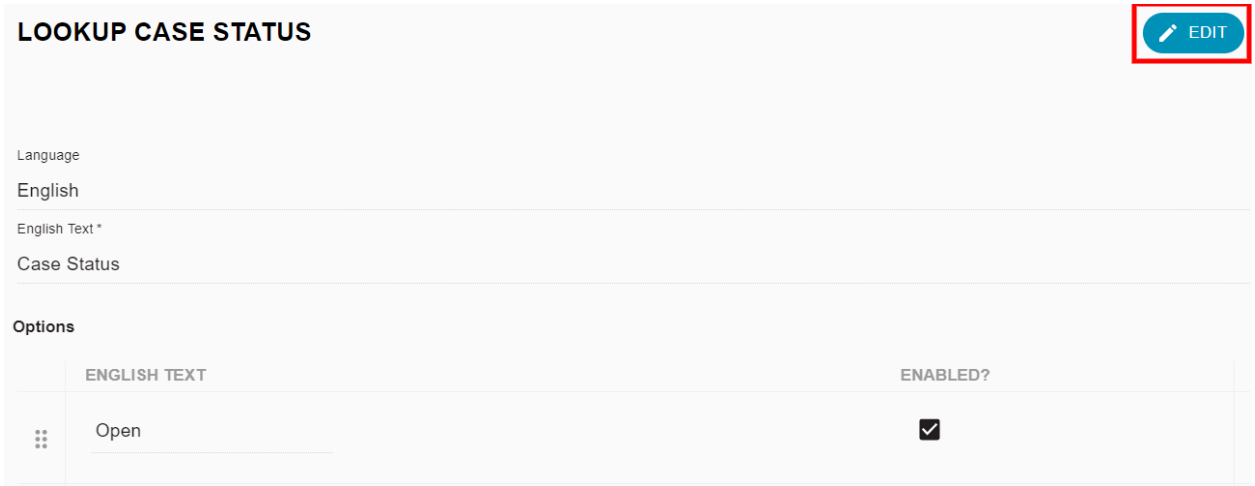


Specify a name for the Lookup you are creating, then use the **Add** button to add options. To add translations for the Lookup name or options, select a language in the “Language” dropdown at the top of the page, then fill in the translation text.

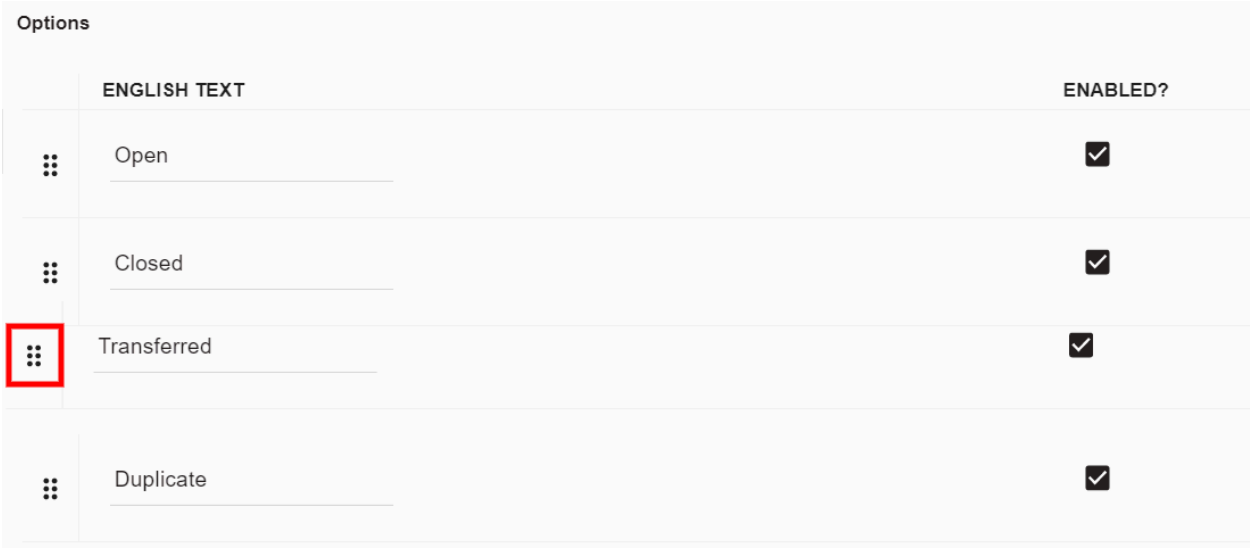


Editing a Lookup

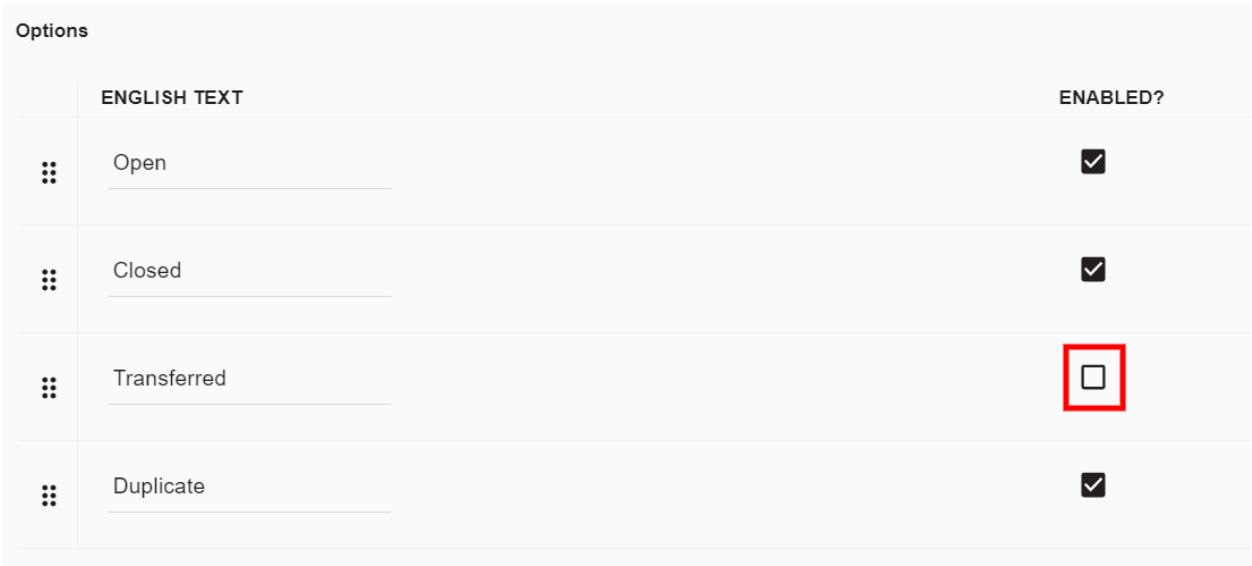
To edit an existing Lookup, go to the Lookups list, click on the Lookup you would like to edit, then, on the Show Lookup page, click **Edit.**



To rearrange the Lookup options, use the “grip” on the left side of the option row to drag-and-drop an option into a new position.



Note: you cannot delete options from a Lookup. Instead, you can “disable” an option. This will prevent users from selecting this option in the future. To do this, un-check the box next to the option in the “Enabled?” column of the Options list.

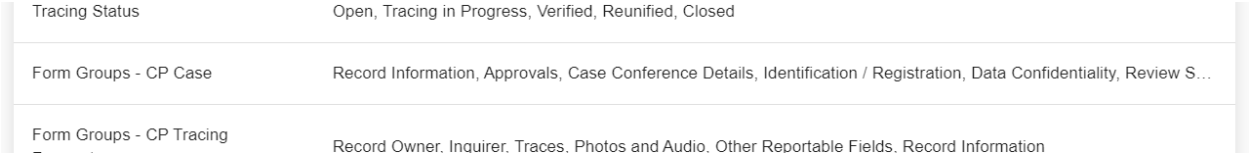


Remember to click the **Save** button after you have finished making changes.

Managing Form Groups

As you scroll through the list of lookups, you will notice that there is a lookup for the form groups for each type of record. In CPIMS+, Find the lookup labelled "Form Groups -

CP Case" you will see that the options include all of the Form Groups see when viewing a CP Case.

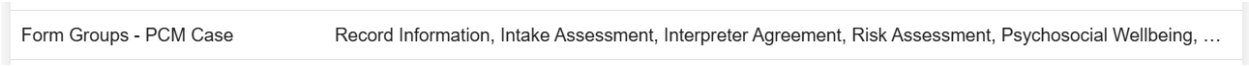


Tracing Status	Open, Tracing in Progress, Verified, Reunified, Closed
Form Groups - CP Case	Record Information, Approvals, Case Conference Details, Identification / Registration, Data Confidentiality, Review S…
Form Groups - CP Tracing	Record Owner, Inquirer, Traces, Photos and Audio, Other Reportable Fields, Record Information

In GBVIMS+, find the lookup labelled "Form Groups - GBV Case" you will see the options include all the Forms Groups see when viewing a GBV Case.

Form Groups - GBV Case	Record Information, Consent For Services, Documents, Consent For Referrals, Safety Plan, Action Plan, Survivor Assessment, Case Closure, Client Feedback, Identificatio…
Form Groups - GBV Incident	GBV Individual Details, Incident, Type of Violence, Record Owner, Alleged Perpetrator, Service Referral, Other Reportable Fields, Record Information

In PCMIMS+, find the lookup labelled "Form Groups - PCM Case" you will see the options include all the Forms Groups see when viewing a GBV Case.



Form Groups - PCM Case	Record Information, Intake Assessment, Interpreter Agreement, Risk Assessment, Psychosocial Wellbeing, …

To update or provide translations for the Form Groups, find the lookup that corresponds to the Module and Record Type of the Form Groups you want to update, click into the Lookup, and click **Edit**. You can now add, update, translate, and reorder the Form Groups the same way you would manage the options for any other Lookup.

Other Important Lookups[a]

There are other Lookups which impact key Primero functionality. Here are a few of them:

- **Service Type -** Updating these options will affect which services you can configure for Agencies and Users, as well as which options appear when you are selecting a type of Service for a Referral.
- **Service Response Type -** Since some implementations use a Case's most recent Service Response Type as its workflow status, updating the **Service Response Type** Lookup may affect which Workflow Statuses appear on the Case and in the Dashboards.
- **PDF Header -** These options appear for users choosing which header to show at the top of their PDF exports. The default values are currently PDF Header 1, PDF Header 2, PDF Header 3, which should be updated to headers agreed by the partners.

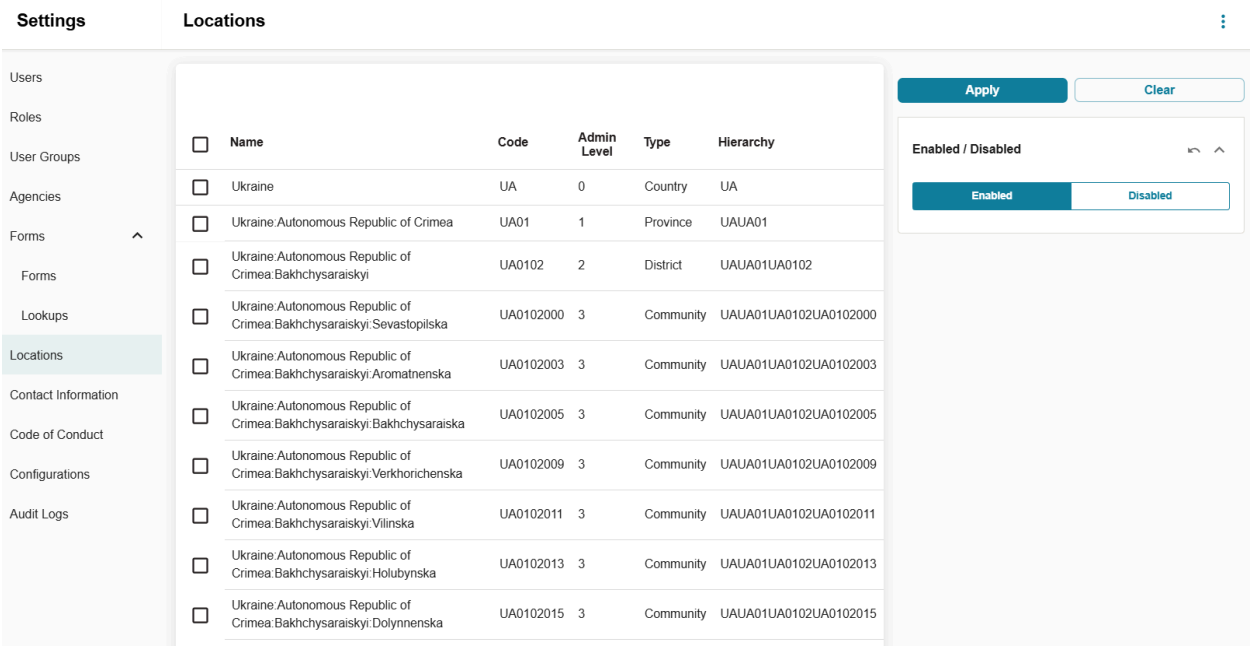
Lookups

PDF Header	PDF Header 1, PDF Header 2, PDF Header 3

- **Agency Office -** Users can be assigned to one of these “Agency Offices.” Supervisors will then be able to filter records by which Agency Office’s users created them.

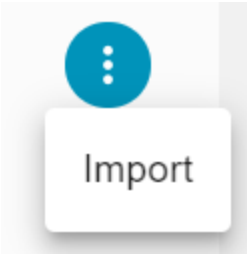
Locations

To view all Locations currently configured in the system, click the **Settings** link in the navigation menu. Then, in the Settings navigation menu, click **Locations.** You will see a list of all system locations.



Importing Locations

To import locations, click the Actions menu at the top-right of the screen, then click the **Import** action.



The Import Locations modal will appear. Here, you can upload the CSV file containing your Locations. Select your file, then click **Import** to begin creating Locations.

Formatting the Locations File

The CSV file containing your locations must be precisely formatted for your Locations to be created properly.

- **UTF-8**: Your file must be encoded using UTF-8. To do this in Microsoft Excel, click “Save As.” In the “Save as type” dropdown, select “CSV UTF-8 (Comma delimited) (*.csv)”.
- **HXL headers**: The second row of your file should contain HXL tags which indicate the Location attribute contained in that column. This tag should contain a designation for both the Location admin level and the Location attribute.
- The highest admin level should be represented by the HXL hashtag “#country”
- Each admin level must contain at least the attributes “name”, and “code”.
- If Locations will need their names translated into languages other than English, include an extra column for each admin level to specify the name in that language.
- For a full reference of HXL tags and how to format them, please see the HXL dictionary: https://hxlstandard.org/standard/1-1final/dictionary/
- **All admin levels represented in each row**: Each row must contain not just the attributes for that location, but for its parent locations.

Below is a sample of the first few rows of a properly-formatted Location CSV file containing place name translations for Jordanian Arabic. **Note:** we strongly suggest uploading 10,000 locations at a maximum in order to not impact performance. Click here to download a template for both CPIMS+, GBVIMS+, and PCMIMS+: https://drive.google.com/file/d/1qHYUs9hgZJ0IuHPJi6I2-VExulnfH65U/view?usp=sharing

Country Code	Country Name	Country Name (Jordanian Arabic)	Governorate Code	Governorate Name	Governorate Name (Jordanian Arabic)	District Code	District Name	District Name (Jordanian Arabic)
#country+code	#country+name	#country+name+ar-JO	#admin1+code	#admin1+name	#admin1+name+ar-JO	#admin2+code	#admin2+name	#admin2+name+ar-JO
JOR	Jordan	الأردن						
JOR	Jordan	الأردن	JOR005	Amman	عمّان			
JOR	Jordan	الأردن	JOR005	Amman	عمّان	JOR005009	Wadi Essier	وادي السير
JOR	Jordan	الأردن	JOR006	Tafiela	الطفيلة			
JOR	Jordan	الأردن	JOR006	Tafiela	الطفيلة	JOR006001	Hasa	الحسا

Updating Locations

Administrators can enable and disable Locations but we recommend the locations that are uploaded must be the final list. When an administrator disables a location, users will then see that location act like a disabled option whenever they are creating or editing a record and using a location field.

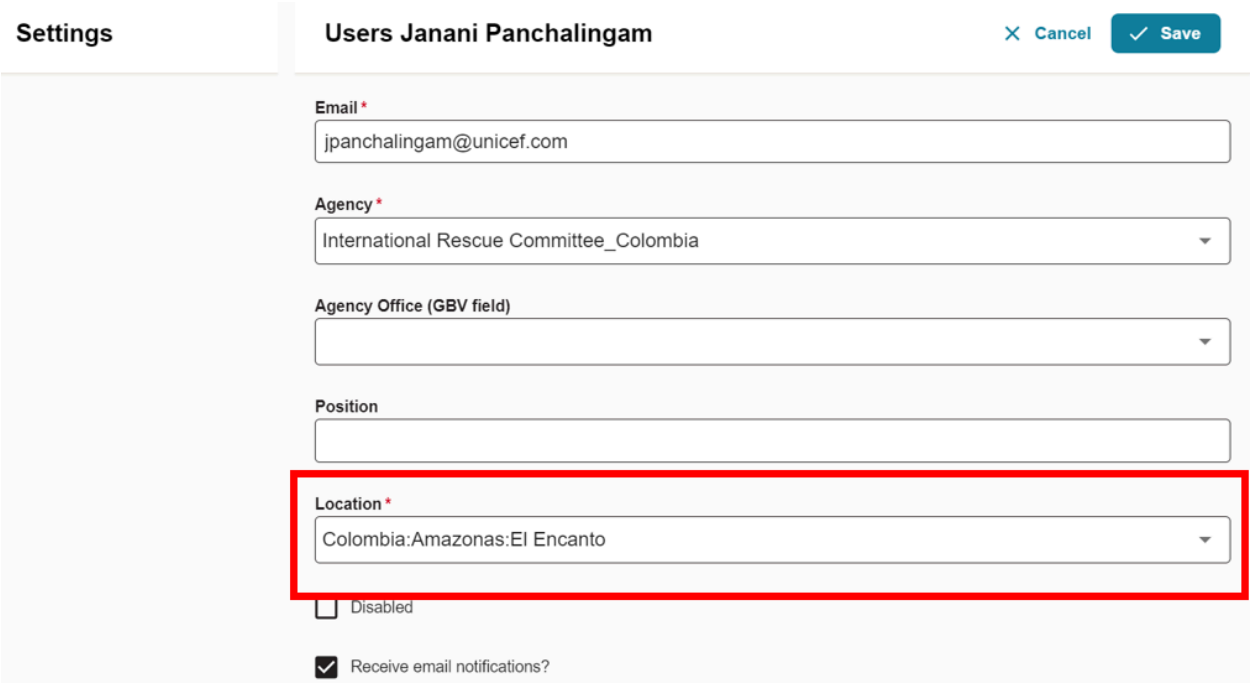
When an administrator enables a location, users should then see that location act like a normal, enabled option whenever they are creating or editing a record and using a location field.

When a user is editing a record where a location was saved in a field, but the location is now disabled, the user will still see the fully-translated location value in the field, but if they de-select that value, they cannot re-select it.

When a user is creating a record or editing a record and clicking into a location field with no previously-selected value, they will not see disabled locations as valued.

Using the Locations

There are many different areas where locations are used within Primero. The below guidance lists the various ways locations are configured and used in the system. Firstly, note that the locations of case workers or managers are selected on their user profile:



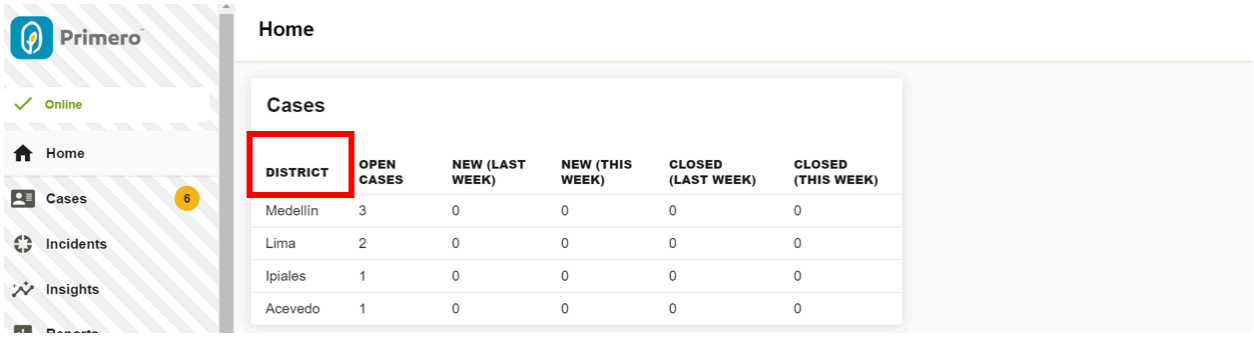
In this example, the location selected is “Colombia: Amazonas: El Encanto”. “El Encanto” is the **district** location, which is administrative level 2.

If the location selected was “Colombia: Amazonas”, this is **county** or **province** location, which is administrative level 1.

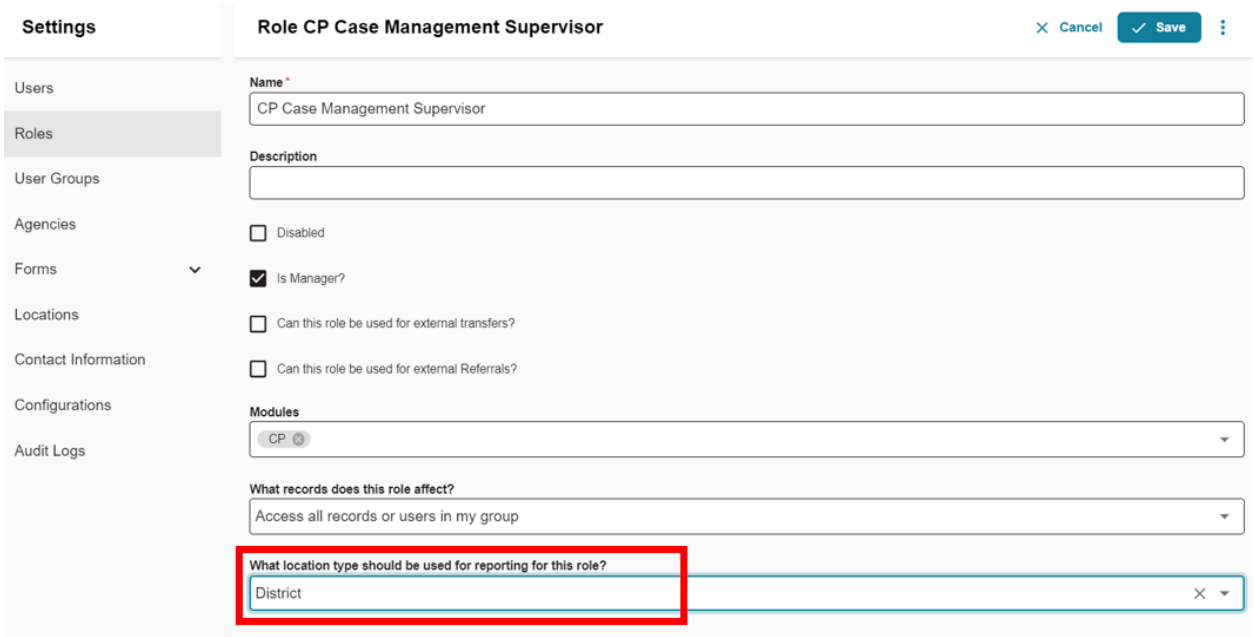
If the location selected was “Colombia”, this is **country** location, which is administrative level 0.

Locations that appear on the Dashboard

When logging in as a system administrator or some managers, you are able to see the cases by a particular administrative level. This is initially set by the developers when the system is set up. In the example below, the system administrator sees the number of **registered cases by district** and this district is determined by the location selected in the case worker's profile:



If a user would like to view the "Cases by Locations" dashboard in a different level from *district* you are to set the location level that appears on the dashboard on the role itself by selecting the level on the question "What location type should be used for reporting for this role?":



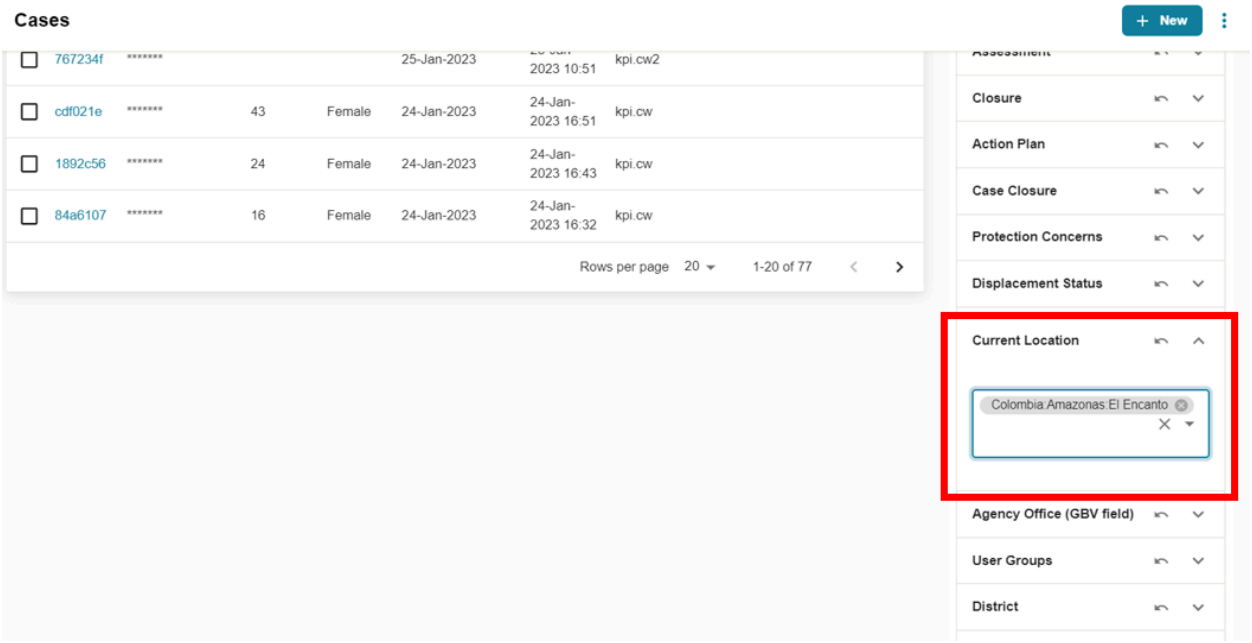
If you select "District" or "Province" then the cases will display by that particular level on the dashboard. ***Please note that if a user's location in their user profile is set to***

"Colombia", then they will not appear in the dashboard because there is no country level dashboard. You will need to ensure all users have the most specific location, such as "Colombia: Amazonas: El Encanto", to be able to appear in both the District and Province dashboard. Users who have "Colombia: Amazonas" will not appear in the District dashboard because the location is not specific enough in their user profile.

If you would like the dashboard to not display registered cases by district, the dashboard can be updated by a developer to display cases by current location. Read more about current location in the next section.

Current Location Filter

When you are on the case list view, you can filter by "Current Location":

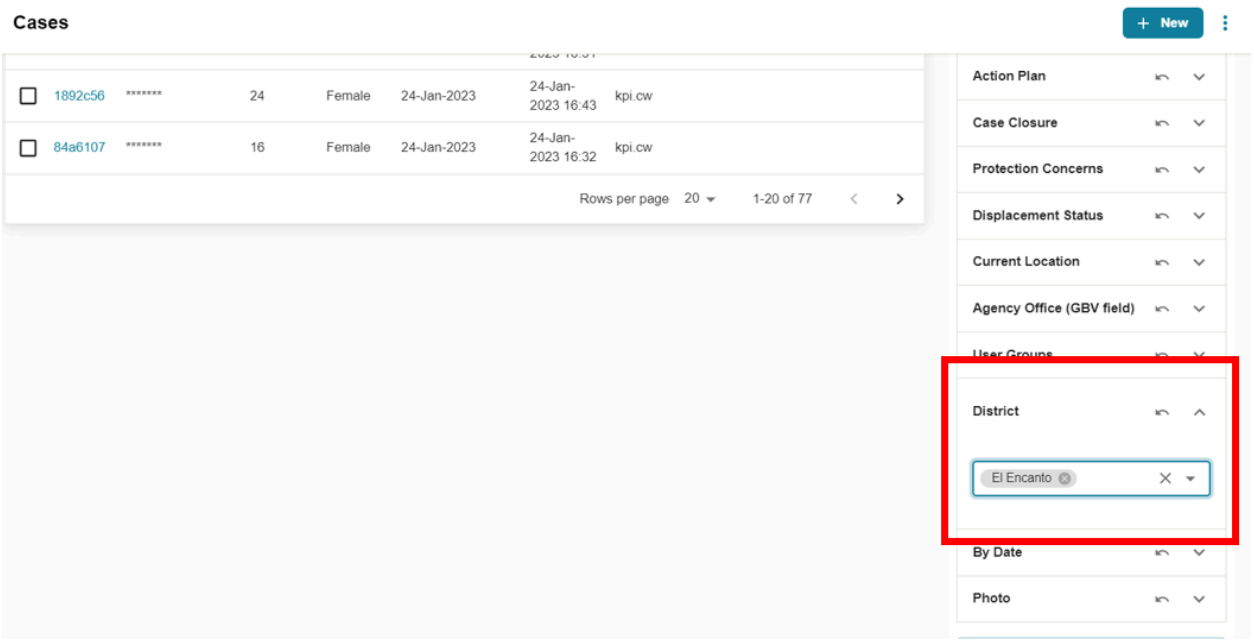


This field is the child's current location and typically on the Care Arrangements form or the Child's Details form under the field called "Current Location" for CPIMS+.

This field is the client's current location and typically on the Intake form under the field called "Geographic location intake" for PCMIMS+.

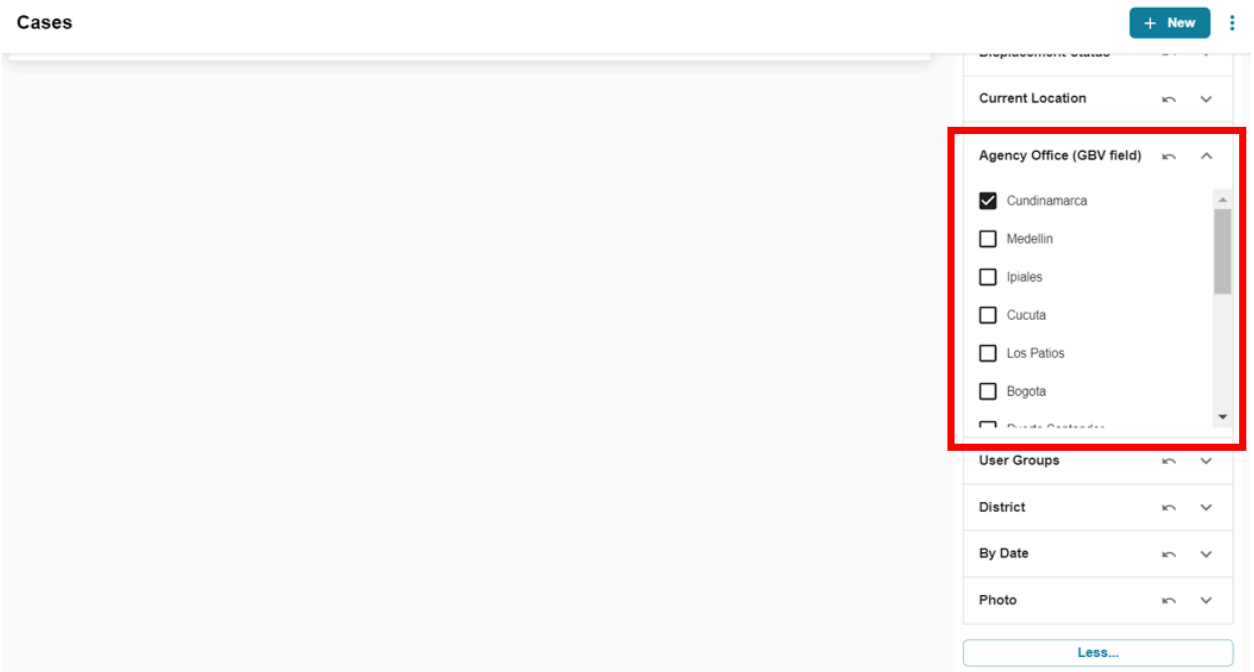
District Filter

When you are on the case list view you can filter by "district" which filters for cases by the case worker's district set on their user profile:

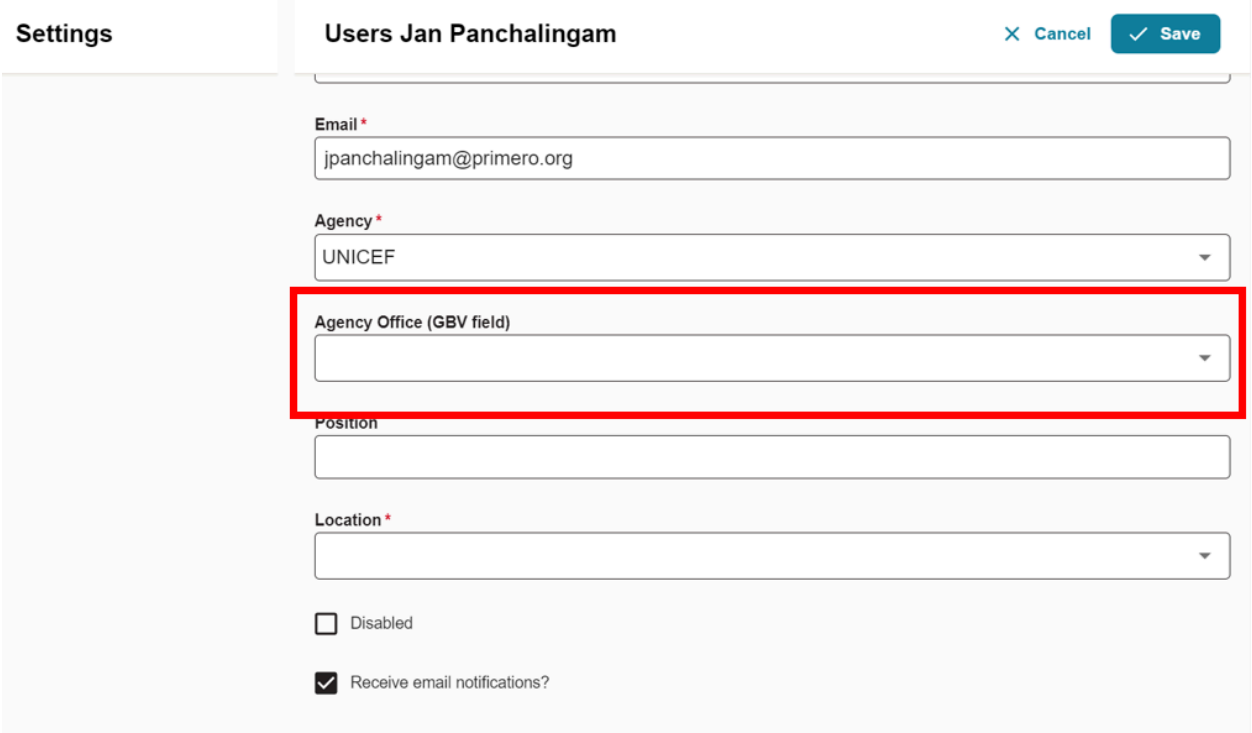


Agency Office (GBV field) Filter

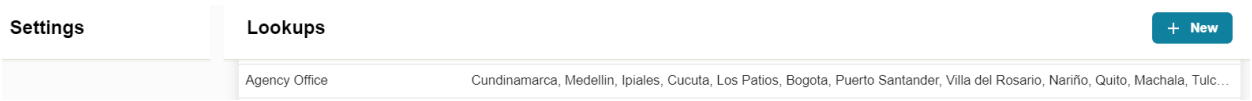
In GBVIMS+, when you are on the case list view, you can filter by “Agency Office (GBV field)”:



This is set by the Agency Office selected on the user's profile and note that this is not the same as the Agency nor does it have a formal link to the Agency in the system:



If you would like to update the list of agency office (GBV field) options, you can update them in the lookup called "Agency Office":



Locations that appear on the reports

Within the reports you are able to generate reports based on the locations listed below:

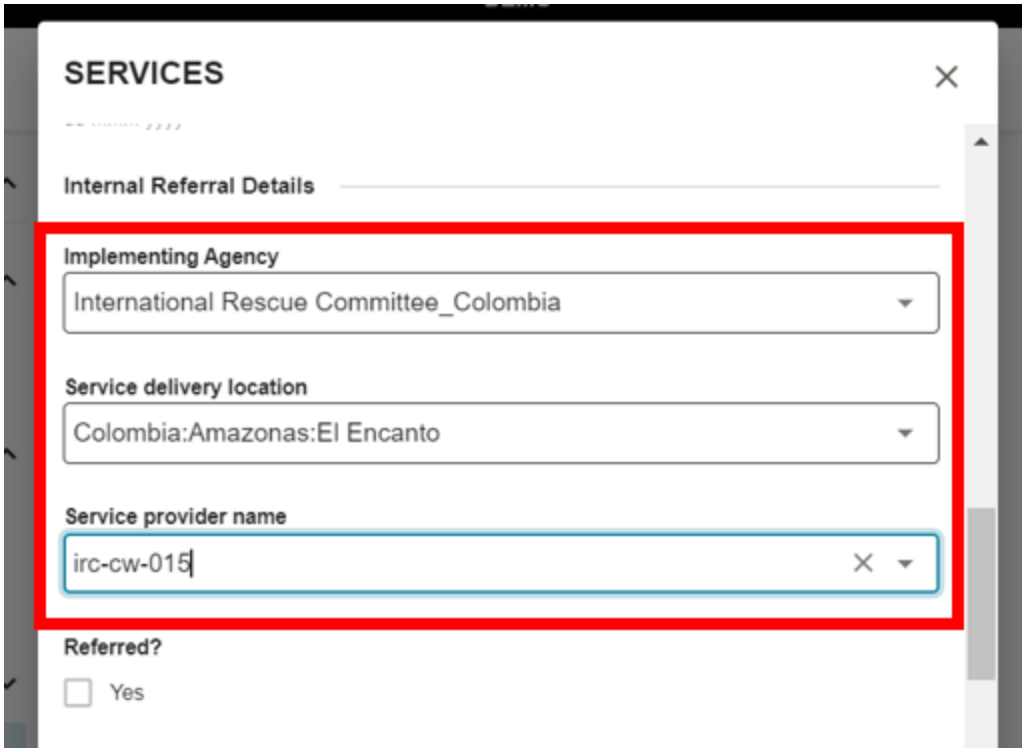
We also are able to generate a report by:

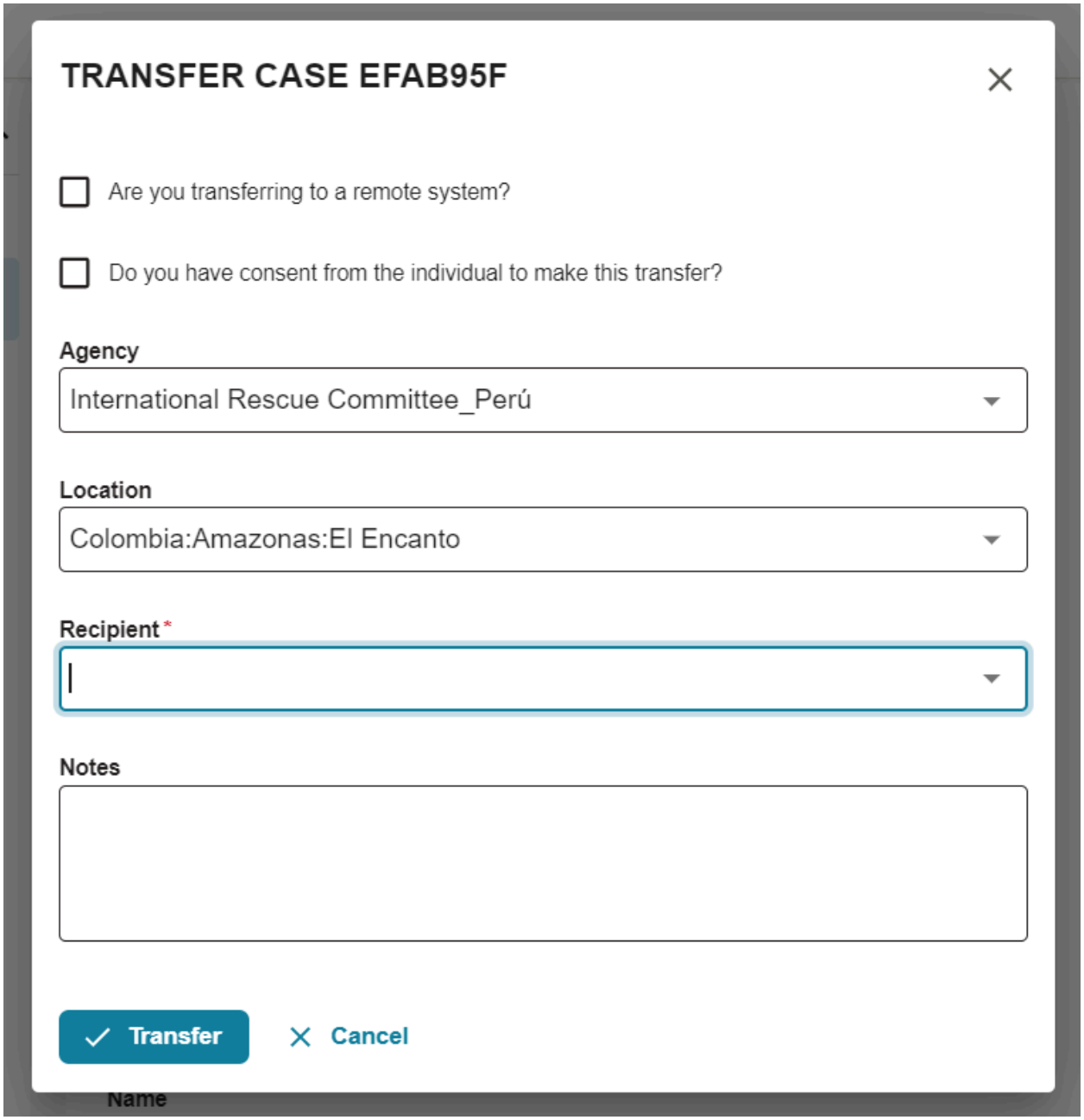
- Created-by user
- Owned-by user
- Created-by user groups
- Owned-by user groups

*Note that "Case Manager's Location" refers to the "Case Worker's Location" or "Record Owner's Location", **not** the supervisor of the case worker.*

Locations when making a referral or transfer

Once a location is selected in an internal **referral** or an internal **transfer**, the users list will be filtered by the province or district of the user. Therefore, if a user is not able to find a specific user, please check their user profile location as well as their agency to ensure the user is correctly set up.


SERVICES
Internal Referral Details
Implementing Agency
International Rescue Committee_Colombia
Service delivery location
Colombia:Amazonas:El Encanto
Service provider name
irc-cw-015
Referred?
Yes



Components of User Management

As described above, each Primero user must have one role and at least one user group, allowing them to access the functions and records necessary to perform their day-to-day work. User management consists of the following three elements:

- **Users** are the individuals using Primero who each have a unique username and password. Each user is given access to one or more modules in Primero (e.g., CP for case management or GBV for gender-based violence case management).

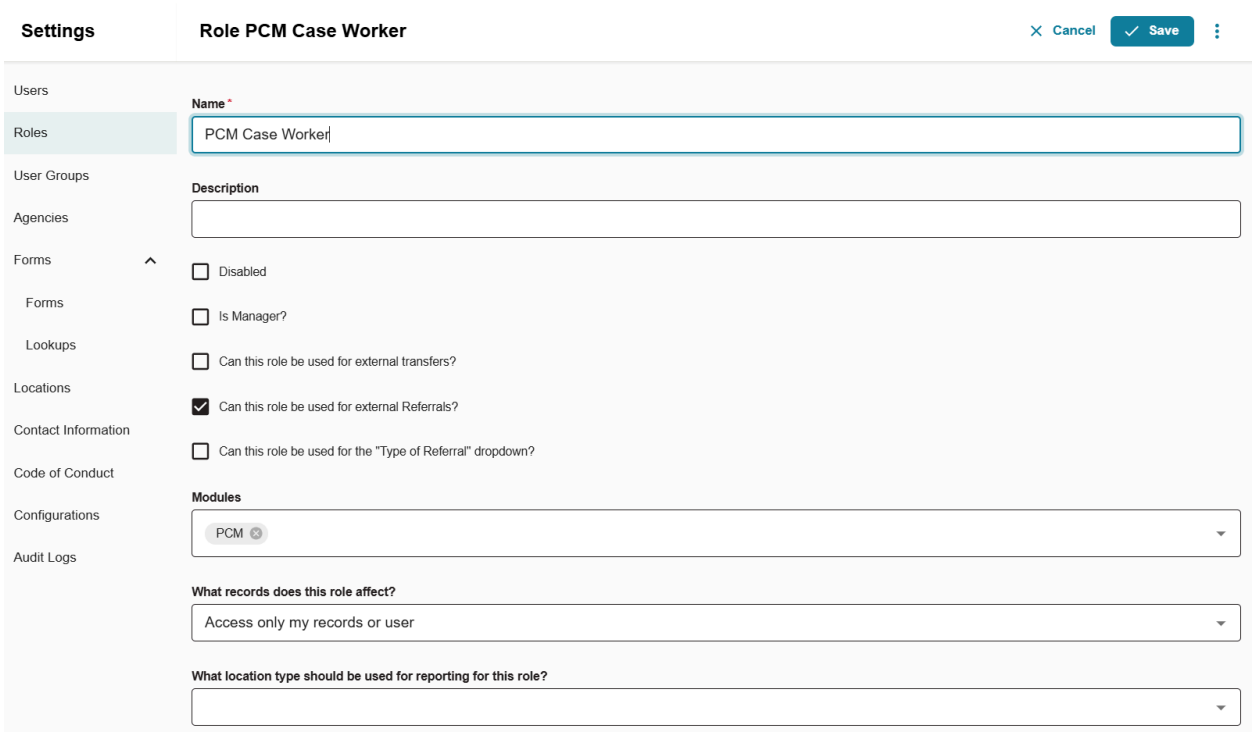
- Their **Role** sets which actions they can perform on which record types; as well as which records they are able to access. Below are some examples to illustrate these two concepts:
    - *Actions*: A role may be able to “View,” “Edit,” and “Flag” Cases, but only “View” Incidents.
    - *Access*: A role may be able to access all records in the system, all records managed within their User Groups, all records managed by their Agency, or only their own records.
- A **User Group** is like a team of users. Supervisors within a User Group will be able to see any records managed by members of the group.
- A user’s **Agency** represents the actual organization they work for. Please note that, while User Groups are not linked to Agencies in any way, an administrator can create multiple User Groups which represent teams within an Agency (example: all Save the Children case workers in District 5). Or, they may create a User Group which spans multiple Agencies (example: all Alternative Care service providers in Camp 1).

Creating and Editing Roles

In the Settings navigation menu, click **Roles**. To create a new role, click the New button, or to edit an existing Role, click a Role in the list, then click the Edit button on the Show Role page.

General Settings

In the first section of the new/edit Role page, you will see the below fields



- **Name:** The name of the role. For example, GBV Case Worker or PCM Organization Focal Point.
- **Description:** A written description of the role and its function.
- **Disabled**: Since you cannot delete Roles in Primero, disabling a Role prevents it from appearing as an option when an administrator creates a User.
- **Is Manager?**: This setting allows Users with this Role to see management-related features such as the “By Caseworker” filter on the Cases list. You should generally select this setting for all managerial and administrative Roles.
- **Can be used for external Transfers?**[b]: Allows this role to appear as an option when a user is selecting the *Type of Recipient* for an external transfer. When a user selects the *Type of Recipient*, the external transfer will only include information that the selected *Type of Recipient* would normally have access to in Primero. For instance, if the user selects “Service Provider” as their *Type of Recipient*, and the Service Provider role only has access to the “Child’s Details” form, the external transfer will only include information contained in this form.
- **Can be used for external Referrals?**: Allows this role to appear as an option when a user is selecting the *Type of Recipient* for an external transfer. When a user selects the *Type of Recipient*, the external referral’s PDF export file will only include information that the selected *Type of Recipient* would normally have

access to in Primero. For instance, if the user selects “Service Provider” as their *Type of Recipient*, and the Service Provider role only has access to the “Child’s Details” form, the external referrals’s PDF export file will only include information contained in this form (if CPIMS+), “Survivor Assessment” (if GBVIMS+), or “Referral Form” (if PCMIMS+).

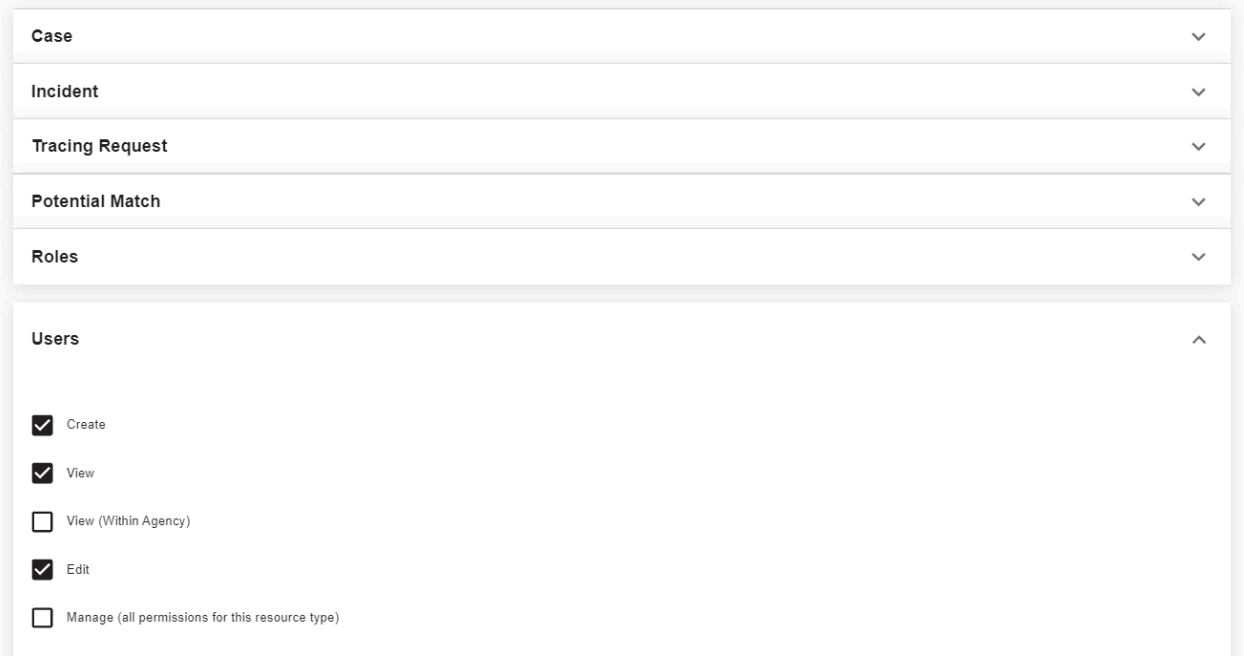
- **Can this role be used for the "Type of Referral" dropdown?:** This allows the role to appear as an option for the “Type of Referral” dropdown when the user performs an internal referral. If the user chooses this role as a type of referral, the referral recipient will only be able to access the forms which the selected role can access in the “Forms” section of the role.
- **Modules:** Which Primero modules will users with this Role have access to? Typically, Roles only have access to one. For instance, a CP Case Worker would only have access to the CP module. For GBVIMS+, a GBV Case Worker would only have access to the GBV module. For PCMIMS+, a PCM Caseworker would only have access to the PCM module. This impacts which forms are available when a User with this Role is creating, viewing, or editing a record such as a Case. **Please ensure this field has a module selected**.
    - ***Note:*** *you must have a module selected to be able to “copy” a role.*
- **What records does this role affect?**: This controls which records Users with this Role will be able to access.
    - This setting has the following options:
        - “Access only my records or user”
        - “Access all records or users in my group”
        - “Access all records or users in my agency”
        - “Access all records or users”
        - "No records - Admin functionality only."
        - Please note that a User will be able to perform their permitted actions for a given type of record for any records of that type which they can access. For instance, if a supervisor role has the *Edit* permission on *Cases*, and they have access to *all records in their group*, they will be able to *edit all Cases in their groups*.

- **What location type should be used for reporting for this role?**: Primero generally uses a system-wide setting for the level of specificity used to report Cases' locations in Dashboards and filters.
    - Let's use Ghana as an example and assume that usually locations in Ghana are classified into one of Ghana's 260 districts. If a user is looking at the "Cases by Location" dashboard and only has access to the Cases in their own region, they will only see a few rows in the dashboard - one for each district in their region. In this case, classifying locations by district makes sense.
    - However, a national administrator, with access to all cases in the system, would see 260 rows in that same dashboard. This is confusing and impractical. In this situation, the National Administrator role should have the "What location type should be used for reporting for this role?" field set to "Region," so that National Administrators only see 16 rows in the dashboard: one for each of Ghana's 16 regions.

Permissions

Scrolling down the page, you will see that a Role's "Permissions" are organized by record type. This includes both the three main record types (Cases, Incidents, and Tracing Requests), as well as record types like "User" and "Report" which pertain to system configuration, and which usually only administrators can access.

Please note that you can expand or collapse the section for a particular resource type by clicking on the header of that section. This makes scrolling through the page easier.

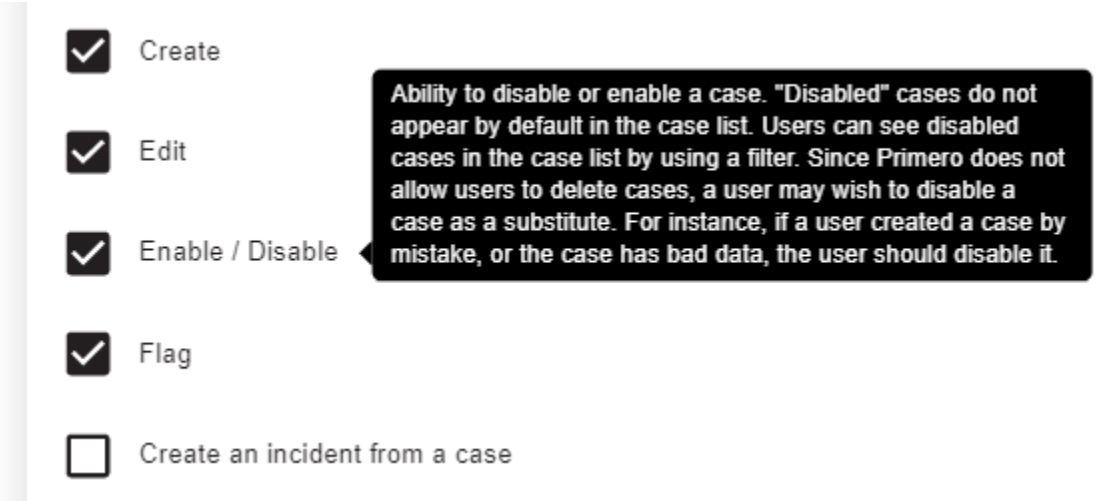


You can update permissions for the following record types:

- **Case**: Represents an individual child, survivor, or other beneficiary.
- **Incident**: Represents an occurrence of GBV which has occurred to the survivor. Incidents should always be linked to Cases. These are usually incidents of abuse or violence, though they can also correspond to events like encounters with law enforcement. Incidents are often linked to Cases. (GBVIMS+ only)
- **Tracing Request**: Represents an individual trying to locate and reunify with an unaccompanied or separated Case. (CPIMS+ only)
- **Potential Match**: Represents the link between a Tracing Request and a Case. Access to Potential Matches is necessary for Family Tracing and Reunification (FTR) work. (CPIMS+ only)
- **Role**: Dictates which actions a User can perform in Primero.
- **User**: Represents an individual User account.
- **User Group**: Represents a team or a collaborative group of users who can share information. Managers can typically see all of the records managed by social workers in their User Groups.
- **Agency**: Represents an organization with members who use Primero. Agencies exist independently of User Groups.

- **Forms, Lookups**: Controls the ability to configure Primero Forms and Fields, as well as Lookup options used within them.
- **System**: Miscellaneous system-wide configuration settings.
- **Report**: Aggregate data analysis tool. Includes table and graph representations of data.
- **Dashboard**: Dictates which summary information appears on the home page.
- **Audit Log**: Filterable list of all actions performed in the system. Does not include any identifiable information on Cases, Incidents, or Tracing Requests.
- **Matching Configuration**: Controls which fields are used to compare Tracing Requests with Cases during Family Tracing and Reunification.
- **Duplicate Search**[c]: Advanced case search for administrators.
- **Pulse / KPIs**: A set of performance-monitoring indicators and dashboards tailored for GBV programming.

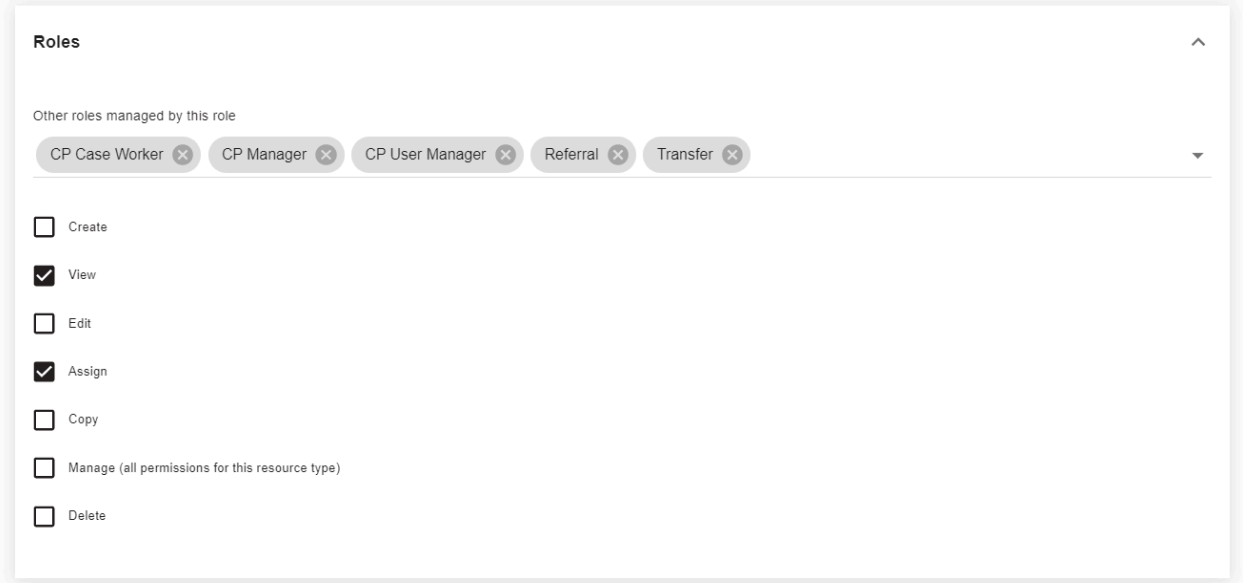
Each resource type has a different set of permissions, each of which represents a specific action that a User with this Role can perform. To see an explanation for a permission, hover your mouse over the text for that permission. A box will appear with a short description. **When in doubt, always check these explanations for guidance on how to configure a Role.**



A few specific permissions warrant explanation here:

- **Roles - “Other roles managed by this role”**: This specifies which other Roles users with this Role can access. For example, if you give this Role the ability to ‘View’ and ‘Edit’ Roles, they will only be able to view or edit the Roles you select

here. For example, to limit what kinds of Users an Organizational Administrator can create, you would give them the “View” and “Assign” permission on Roles, but you could select the “Case Worker” and “Supervisor” Roles in this field to specify that Organizational Administrators can only create users with these two Roles. This prevents the Organizational Administrator from creating a user account with a very powerful Role such as “National Administrator.”



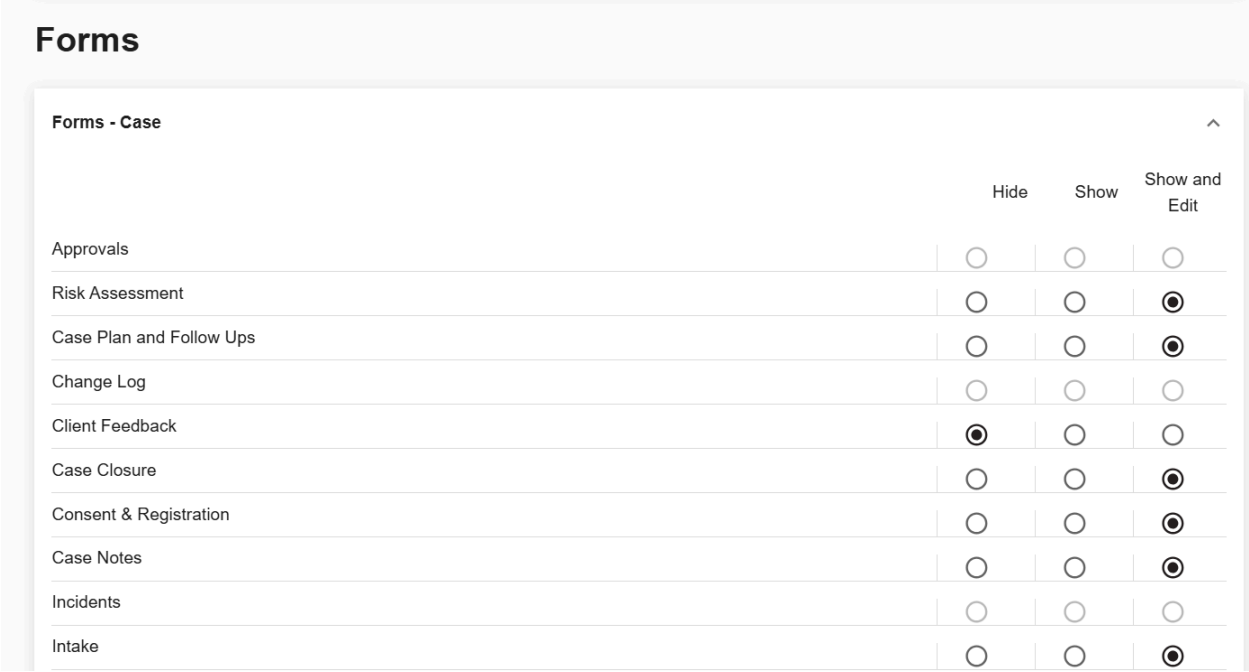
- **Dashboard - “Tasks Page”**: Rather than controlling access to a specific “dashboard” within the home page, this permission gives Users with the Role access to the separate “Tasks” page, where users can keep track of upcoming case management deadlines. For more information on this view, see the **Primero CPIMS+ User Guide** or Primero GBVIMS+ User Guide.
- **Users - “View (Within Agency)”**: This denotes that the given role can perform actions on Users only within the current User's agency. As an example, suppose an administrator named Ahmad at a local NGO named "ABC" needs to be able to manage the organization's Users: resetting passwords, disabling Users, and creating new User accounts. Ahmad's User account gets a role with the “Edit,” “Assign,” and “View (Within Agency)” permission for Users. Because of this, Ahmad will only be able to view and edit User accounts which, like Ahmad's User account, have their agency set to "ABC." This means Ahmad can only access, and is only responsible for, Users within his organization.
- **Reports - “Group Read”**: Typically, when a User views a Report, the numbers they see will reflect all records in the system, *regardless of which records that User*

actually has access to. For instance, a User with no access to Cases can still view a Report which includes information about all Cases in the system. However, Users whose Role has the “Group Read” permission on Reports will see numbers in each report will reflect *only those records which are accessible to users in the current user's user groups*. This permission is often used for local, regional, or agency administrators.

- **(Multiple resource types) - “Manage”** - The “Manage” permission appears on multiple types of resources and generally means “All of the above.” If a Role is given the “Manage” permission on a resource, it will be able to perform **all available actions** on that resource.

Form Access

Scrolling down the page, you will arrive at the “Forms” section. Here, you specify which forms this Role will have access to for each of the three main record types: Cases, Incidents, and Tracing Requests.



This dictates which information a Role can access and modify. For instance, Roles with the “Show and Edit” permission on Cases, and with access to the “Child’s Details” form will be able to edit information for any field contained in this form. Roles with “Hide” permission, will not be able to view the “BID Status” form. Roles with “Show” permission will be able to view but cannot edit the “Assessment” form.

Please note that you can expand or collapse the sections for each record type (e.g. “Forms - Case”) within the Forms section by clicking on the header of the section.

Other restrictions on Administrative Roles

Superusers and User Admins

There are two important types of roles which we must discuss here, since the system treats them differently. The first is the **Superuser** role.

A **Superuser** role is a role has the all-encompassing "manage" permission for **Cases**, **Incidents**, **Reports**, **Roles**, **Users**, **User Groups**, **Agencies**, **System Settings**, and **Forms and Lookups**. A superuser, meanwhile, is a user who has been assigned such a role. Since this user has a great deal of power within the system, only superusers can view or edit the attributes of other superusers. For similar reasons, superuser roles cannot be edited within Primero's administrative interface.

The second special type of role is the **User Admin** role. A user admin role has less power than a superuser role but is defined as having the all-encompassing "manage" permission for **Roles**, **Users**, **User Groups**, **Agencies**, **System Settings**, and **Forms and Lookups**. Once again, a user admin *user* is a user who has a user admin *role*. Only superusers and other admin users can view or edit the attributes of user admin users. Similarly, only superusers can edit a user admin role.

Please note that Superusers are never enabled except for situations of emergency maintenance and support.

Note: *As a security measure, admins will not be able to access roles they create and the Primero team will need to provision the access to any newly created roles. If the programme team does not agree with this security measure, the Primero team can remove the role access permission so this does not become an impediment in the programme.*

User Groups

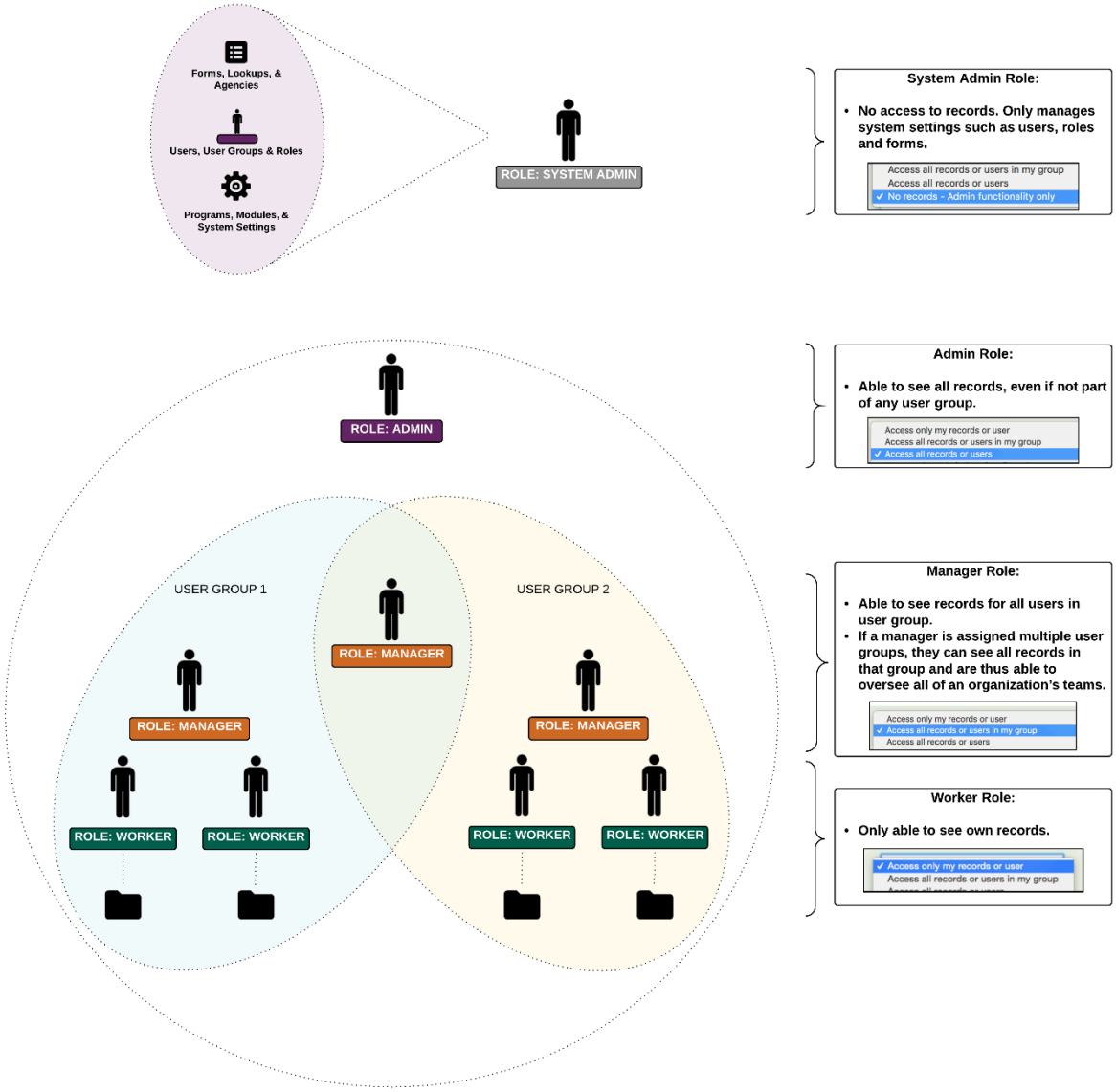
User Groups are teams of users. Users within this group with managerial Roles will be able to access all the records managed by the other users in the group. As with Roles, User Groups should be created before you create individual users. As we discussed in the **Creating and Editing Roles** section, each role has one of the following “access” levels:

- Access only my records or user
- Access all records or users in my group

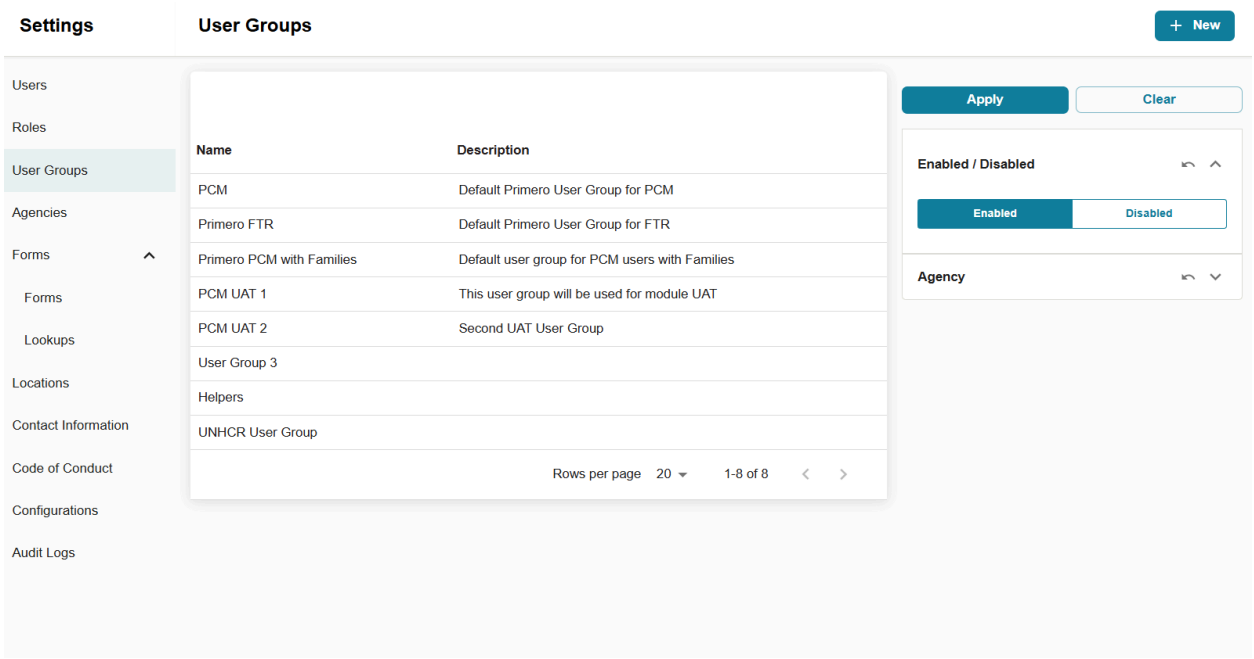
- Access all records or users in my Agency
- Access all records or users
- No access - Admin functionality only

The actions the user can perform once they have access to a record are driven by the privileges set with their role. These permissions given to a user apply to all records they have access to. If a user has the “Edit” permission on Cases and also happens to have access to the Cases of all the Users in their User Group, then they will also be able to edit the Cases of all the Users in their User group.

The following diagram helps explain the relationship between Users, Roles, and User Groups through a hypothetical Role/User Group setup, where the different roles are given specific permissions regarding their ability to see records within different User Groups:



To see the User Groups currently configured in your system, click the **Settings** link in the navigation menu, then click the **User Groups** link in the Settings navigation menu. You will arrive at the User Groups list.



Limited Access to User Groups

Note that local administrators who manage the User accounts for their team will only see User Groups in this list *which they are part of*. Similarly, when this local administrator creates or updates a User account, they will only be able to assign a User to the User Groups that the local administrator is part of. This specifically applies to Users whose Roles have the “All records or users in my group” access level.

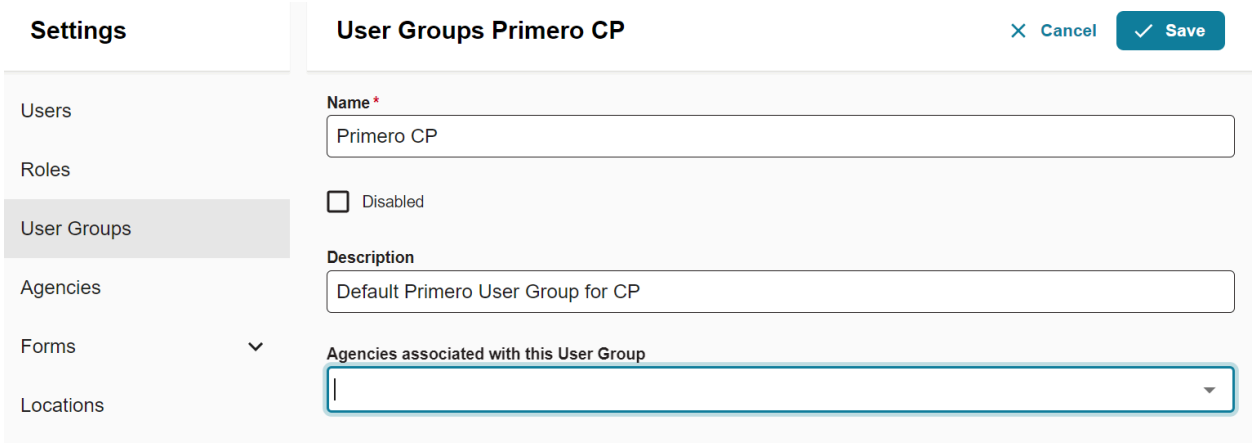
For example, imagine a User with the “Camp Supervisor” Role manages User accounts for all the User Groups in Camp 1. The “Camp Supervisor” Role would have the “All records or users in my group” access level, and this Supervisor User would be part of all the User Groups for Users in Camp 1 (for example: “Camp 1 Block 1,” “Camp 1 Block 2,” and “Camp 1 Block 3”). When this supervisor goes to the User Groups list, they would only see these three User Groups, and when they created a User account, they would only be able to assign the User to one of these three User Groups.

Creating and Editing User Groups

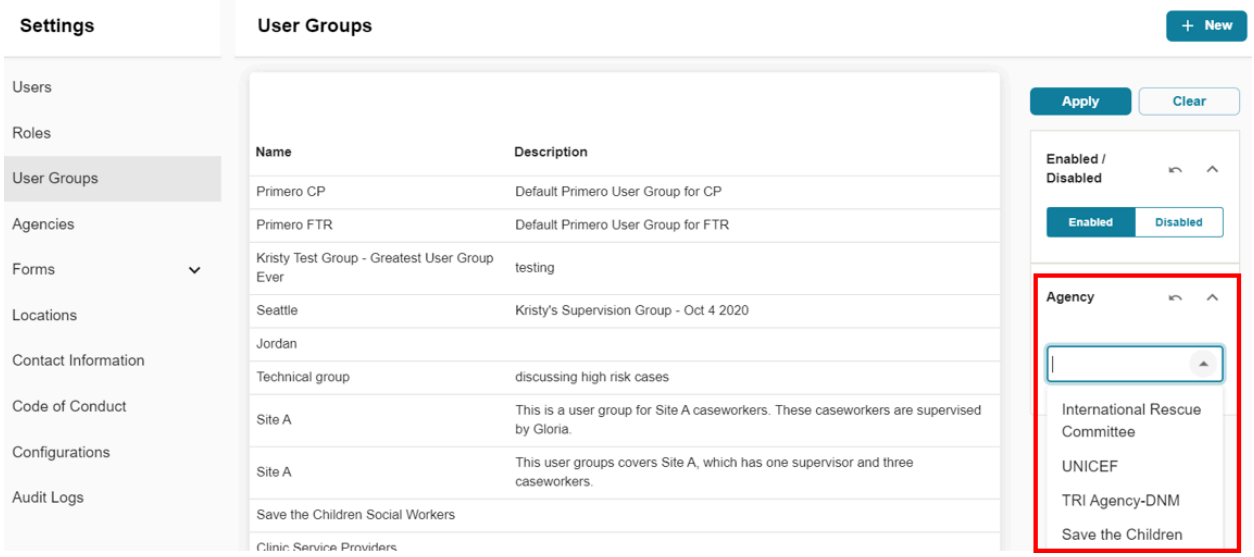
To edit a user group, click one in the list. Once you have reached the Show User Group page, click the **Edit** button. Make changes, then click **Save.**

To create a new user group, click the **New** button at the top of the User Groups List page. Specify a Name and Description, then click **Save.**

Please note that User Groups cannot be deleted. To prevent a User Group from being assigned to Users in the future, or to prevent it from appearing in filters, dashboards, or Reports, edit the User Group and check the "**Disabled?**" tick box.

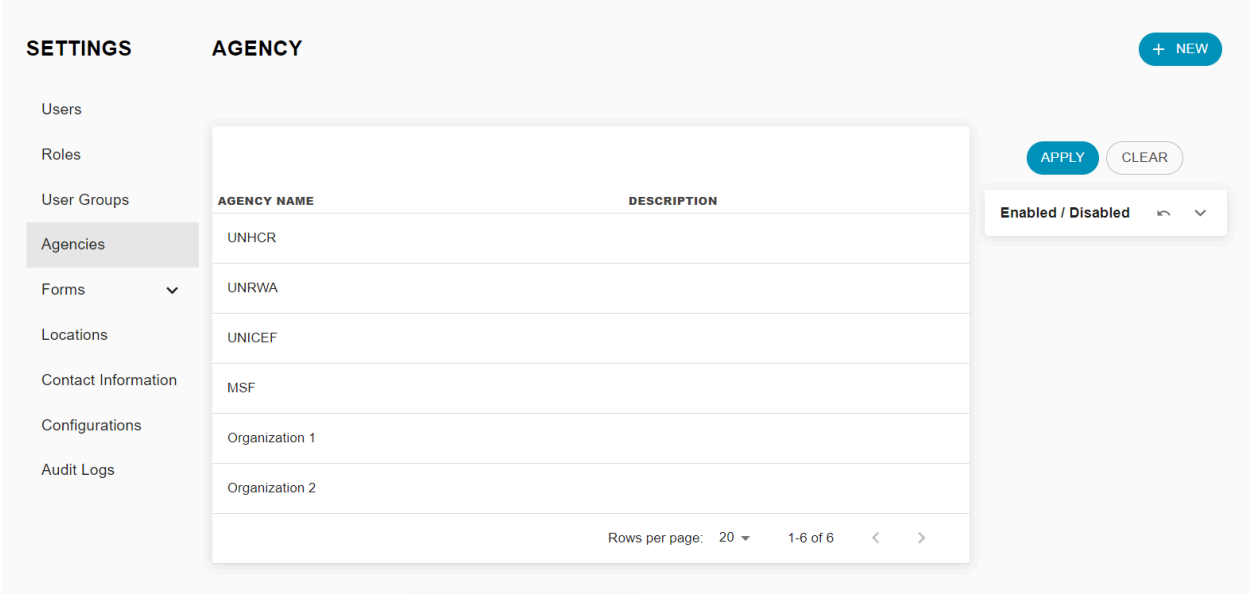


You can add "Agencies associated with this user group". This will not impact any specific functionality. It will allow you to filter by agency in the "User Group" list view:



Agencies

Agencies represent the actual organizations using Primero. You must set up Agencies before creating User accounts. To view the Agencies currently configured in your system, click the **Settings** link in the navigation menu, then click the **Agencies** link in the Settings navigation menu. You will arrive at the Agencies List page.



Please note that Agency Administrators, whose Roles have the “View (Within Agency)” permission on Users, will only see their own Agency in this list. Similarly, when they are creating new User accounts, they will only be able to assign a User to their own Agency. For more information on this restriction, please see the **Permissions** section under **Creating and Editing Roles**.

Creating and Editing Agencies

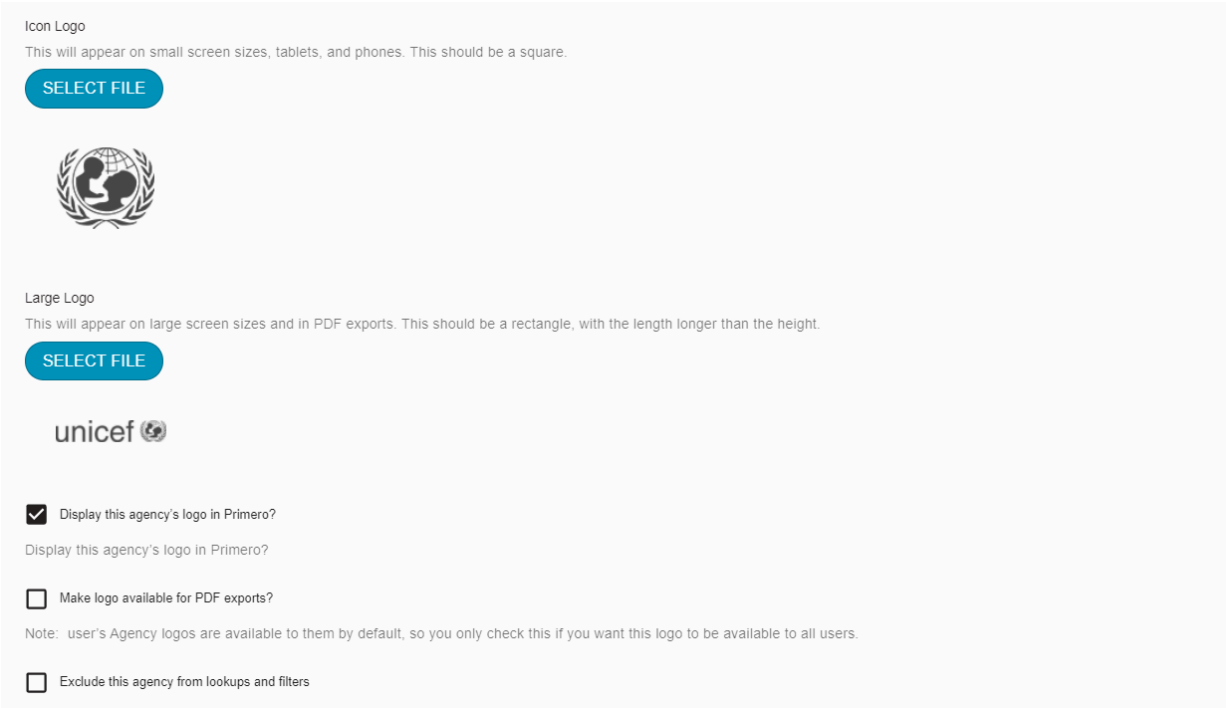
To edit an existing Agency, click the Agency in the list. Then, on the Show Agency page, click **Edit.**

To create a new Agency, click the **New** button at the top of the Agencies List page.

Agency Logos

You can configure an Agency with logo images. If you would like to have the logo appear, you must upload two images:

- An “**Icon**” logo with square proportions. This appears on phone and tablet screens.
- A “**Large**” logo with wide, short, rectangular proportions. This appears on large screen sizes and in PDF exports.

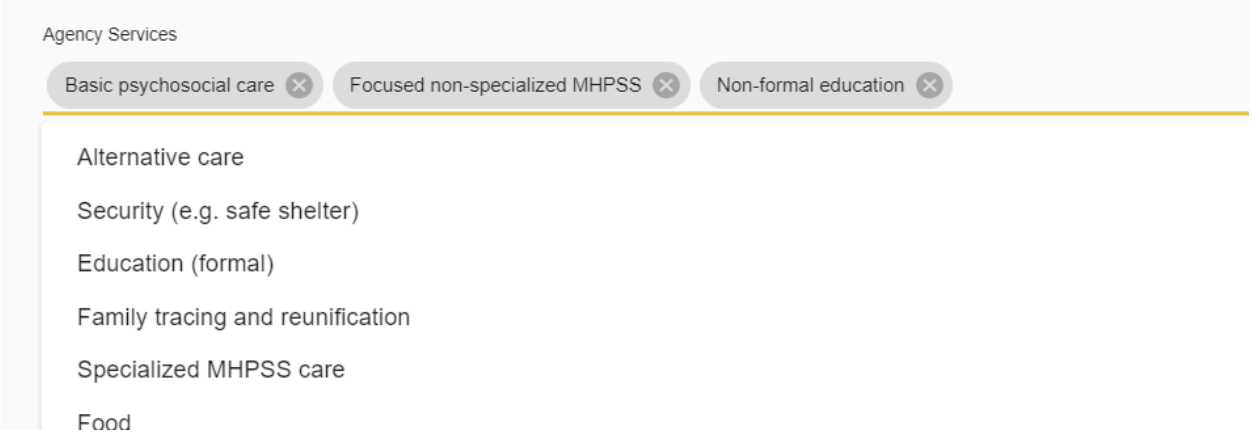


In addition to specifying which images to use for an Agency's logo, you can choose where these logos appear using the below settings:

- **Display this agency's logo in Primero? -** Checking this box will make the Agency logo appear in the navigation menu and on the Login page.
- **Make logo available for PDF exports? -** If this box is checked, users performing PDF exports will be able to select this Agency's logo to appear in the export file's header.
- **Exclude this agency from lookups and filters -** This setting is for Agencies which do not have any Users in Primero. For instance, if you would like to display the logo of your country's Ministry of Justice in the navigation menu or in PDF exports, but no Ministry of Justice staff will actually use Primero, you can create a "Ministry of Justice" Agency, configure its logos, then check this box to ensure that Users do not accidentally select "Ministry of Justice" as the Agency for a referral or transfer.

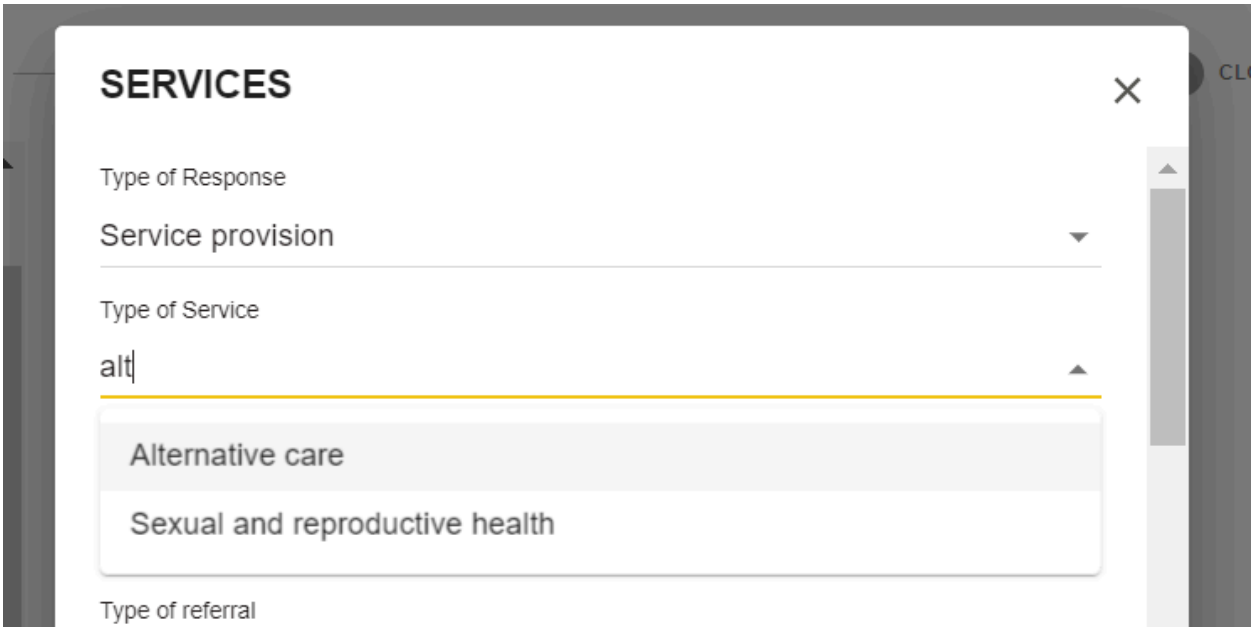
Agency Services

Each Agency can be configured with a list of Services it provides. The options which appear here come from the **Service Type** Lookup.

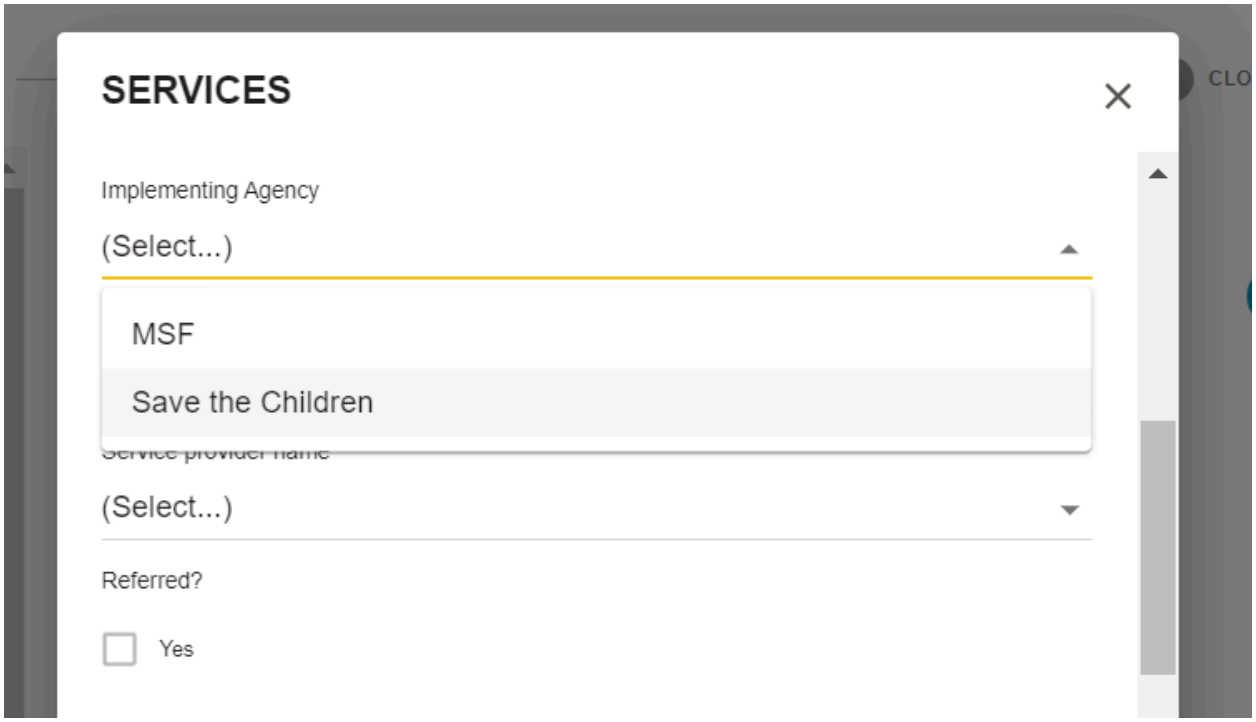


Specifying services for your Agency is very important for controlling the Service and Referral workflow in Primero, as explained below:

- When a user adds a Service to their Case, they will first specify the **Type of Service**.



- Once the user has selected the Service, they will choose an Agency to provide the Service. Primero will only let the user select an Agency which has been configured to provide that Type of Service. So, if the user has selected “Alternative Care” as their Type of Service, and Save the Children is configured to provide “Alternative Care” Services, then Save the Children will appear as an option for the **Implementing Agency** field. Other Agencies, which are not configured to provide “Alternative Care” services, will not even appear as options.



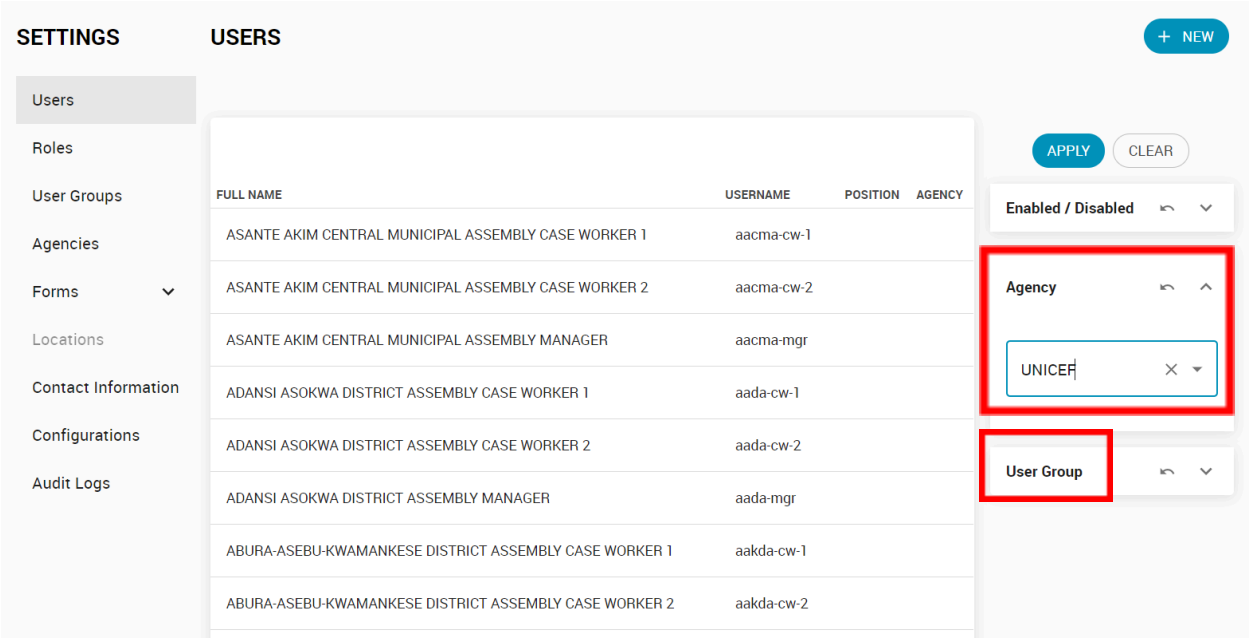
- Once a user has selected a Service Type and an Agency, they can select a User to perform the service. Primero will only show Users who are part of the selected **Implementing Agency**, and which are configured to provide the selected **Type of Service**.
- While we will discuss how to configure which Services a User can provide in the **Creating and Editing Users** section of this guide, it is important to know that an Agency's configured Services can impact which services a User provides. If an administrator, creating a User account, does not specify which Services the User can provide, *Primero will automatically configure that User to be able to provide the Services of their agency.* So, for instance, if Save the Children is configured to provide "Alternative Care" and "Food" services, and an administrator creates a Save the Children User without specifying a list of Services for that User, Primero will automatically configure that User to be able to provide "Alternative Care" and "Food" Services.

Once you are done making changes, please remember to click the **Save** button at the top of the page.

Note: *Once an agency has been created, it cannot be deleted. The agency can only be disabled. To do this, edit the Agency, check the "**Disabled?**" tick box, then save.*

Users

To see all users currently in the system, click on the **Settings** link in the navigation bar, then click the **Users** link in the Settings navigation menu. You will now arrive at the Users List page. You can filter users by Agency, User Group, and whether or not they are Enabled, using the filters panel on the right side of the page.

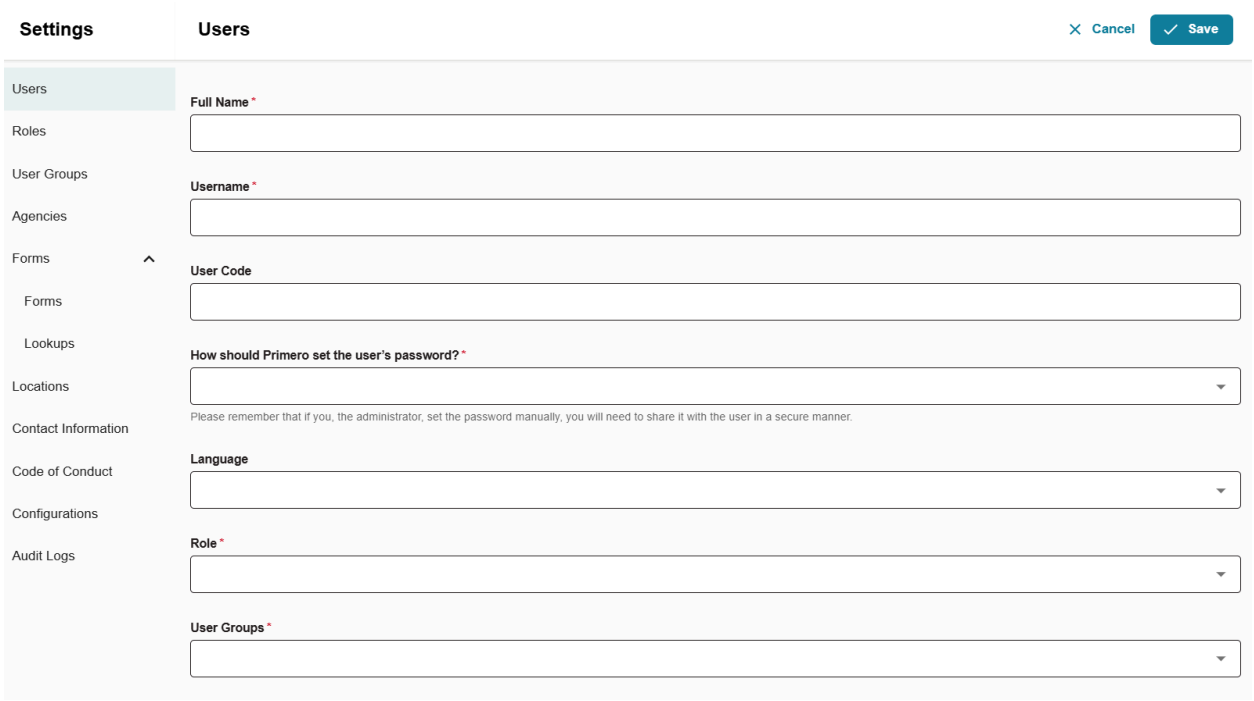


Note that local administrators and supervisors will likely only see Users in their own User Groups or Agency.

- Users whose roles have the “Access all records or users in my group” level of access will see all Users in their User Groups.
- Users whose roles have the “View (Within Agency)” permission on Users will see only Users within their own Agency.

Creating Users

To create a new User account, click the **New** button at the top of the Users List page.



For each user, you must specify the following information:

- **Full Name** - This is the actual name of the User.
- **Username** - Users will enter this every time they login. For this reason, it is recommended to keep the username short.
    - Each User's username should be unique.
    - In addition, the username will be visible on any records created by the User. For this reason, implementation partners should discuss a consistent username pattern. This can include an Agency abbreviation, some indication of the User's day-to-day work (e.g. including 'cw' for case workers), and/or some part of the User's actual name. As partners discuss a pattern, they should attempt to balance the need for Users to be able to understand which person they are dealing with when they read a username; with the need to avoid revealing too much personally identifiable information about the User.
    - Note that if your implementation uses Identity Providers to handle User accounts, the username will need to match a specific format. For more information, please see the **Managing Identity Providers** section of this guide.
- **User Code** - This attribute is not used in most implementations. Unless your configuration is using the User Code to generate composite record IDs, you can ignore this.

- **How should Primero set the User's password?** - Here, you have two options:
    - "I will set the password" - If you select this option, you will be asked to enter the password, then confirm it (to guard against typos). You will then be responsible for communicating this password to the User.
    - "User will set the password using the welcome email" - If you select this option, you do not need to set the password. A password reset email will be sent to the User, and they will be able to set their own password.
- **Language** - The language in which the User will see Primero.
- **Role** - Must be an existing role as defined in the section above. This controls both the User's permissions and level of record access. For more information, please read the **Roles** section of this guide.
- **Modules** - A user is given access to one or more modules in Primero. For example, a Child Protection Officer will likely only have access to the CP (or "Child Protection") module. And a GBV Case Worker will likely only have access to the GBV (or "Gender-Based Violence") module. A Protection Case Management Case Worker will only have access to the PCM module (PCMIMS+).
- **User Groups** - Must be an existing user group or groups as defined in the section above. For managers, this will determine which records they can access. For more information on how User Groups influence which records a User sees, please read the **User Groups** section of this guide.
- **Agency** - The organization to which the user belongs.
- **Location** - The location where the user is based. Please note that this will be used for:
    - *Reporting*: All records created by the User will be listed as being created in this Location
    - *Referrals*: When a User is creating a Service for their Case or performing a Referral, they can filter Users by Location to find a User who is close to them.
- **Services** - The services which the user is capable of providing. Note that this will be used to determine whether this User appears as a potential recipient when other Users are planning Services and Referrals. If you leave this field blank, the User will automatically be given the Services their Agency is configured to provide.

- **Phone** - While this does not currently affect any Primero functionality, it can help administrators and supervisors contact the User.
- **Email** - Welcome, password reset, and notification emails will be sent to this email address. Note that emails are enabled on both demo and production environments.
- **Position** - This does not affect any Primero functionality. The “Position” of the user is meant to capture the User’s precise job title, which may not be properly explained by the Role the User has been given.

Note: *Since a User’s* ***Location****, and* ***Services*** *settings are used to determine whether a User appears as a potential recipient for a Service or a Referral, it is important that administrators regularly update users' accounts to reflect any changes to the Services they provide or their Location. For more information on the Referral workflow, please see the* ***Agency Services*** *section of this guide.*

Note: *If no email exists, then the administrator will select “I will set the password” in the user profile and in the email that can be entered in the user profile is "their username"@”instance URL” so it would look like: jpanchalingam@newyork.primero.org*

Editing Users

To edit an existing user, click on the User in the Users List. Then, on the Show User page, click the **Edit** button. Editing a User account is mostly the same as creating one, with the exception that you cannot update a User’s username once their account has been saved.

Once you are done making changes, please remember to click **Save.**

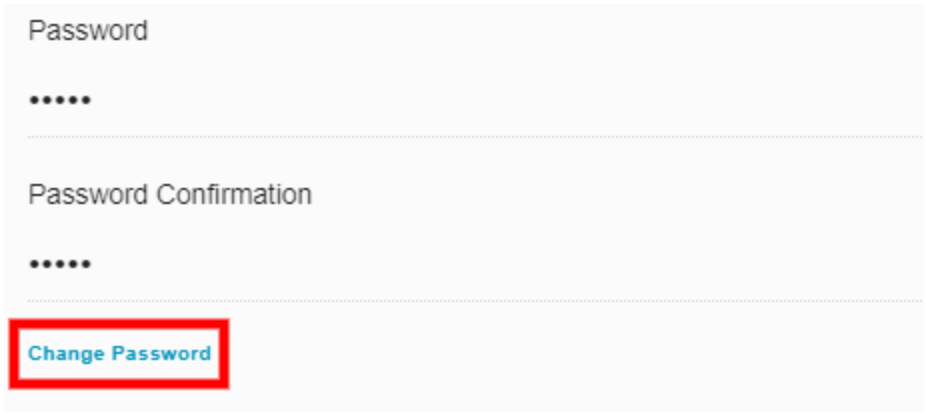
Limitations on editing your own account

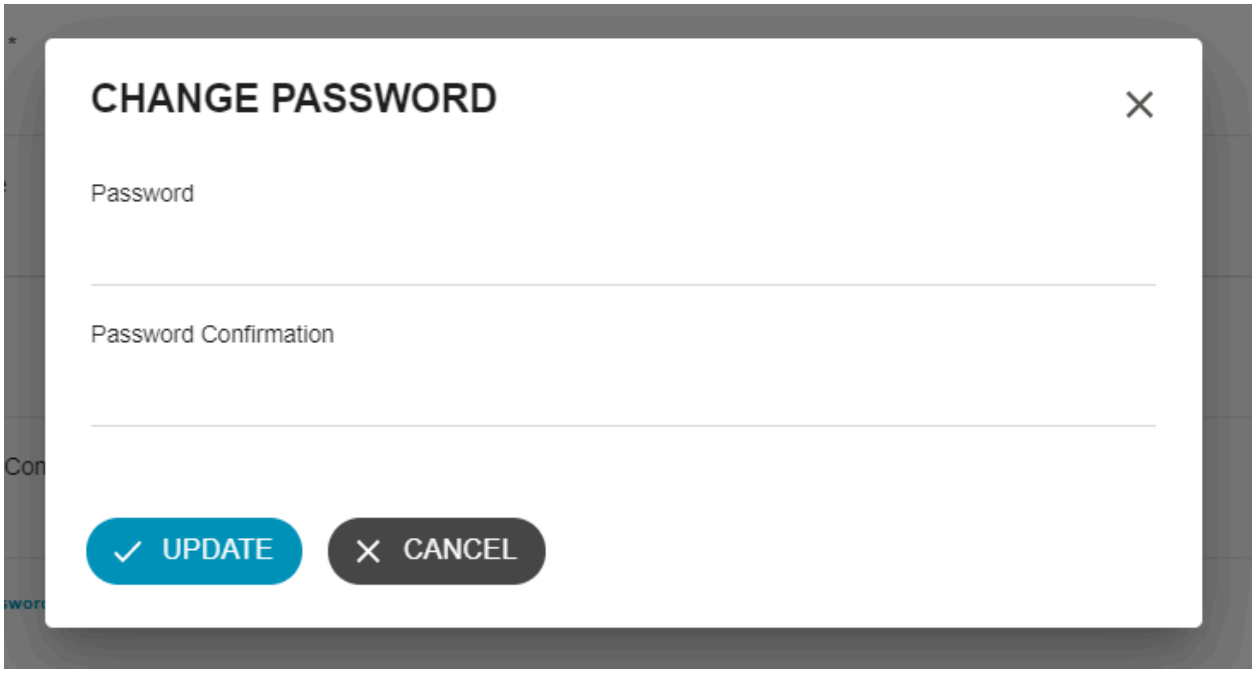
Please note that, while users may sometimes be able to edit their own user accounts, no user may edit which role, user groups, modules, or agency are assigned to their user account. Primero uses this precaution to ensure users do not grant themselves additional power and endanger the data confidentiality of clients.

Updating Passwords

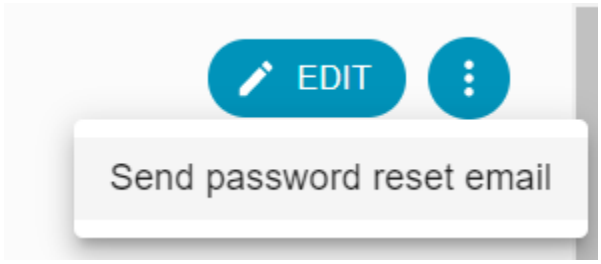
There are two ways to update a User’s password.

- **Edit the account:** When you edit a User’s account, click the **Change Password** link. A modal will appear. Enter the User’s new password, then confirm it. Click the **Update** button at the bottom of the Change Password modal, then click **Save** on the Edit User page.

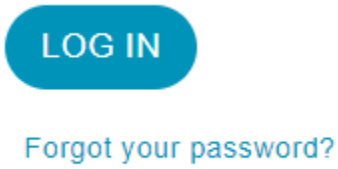




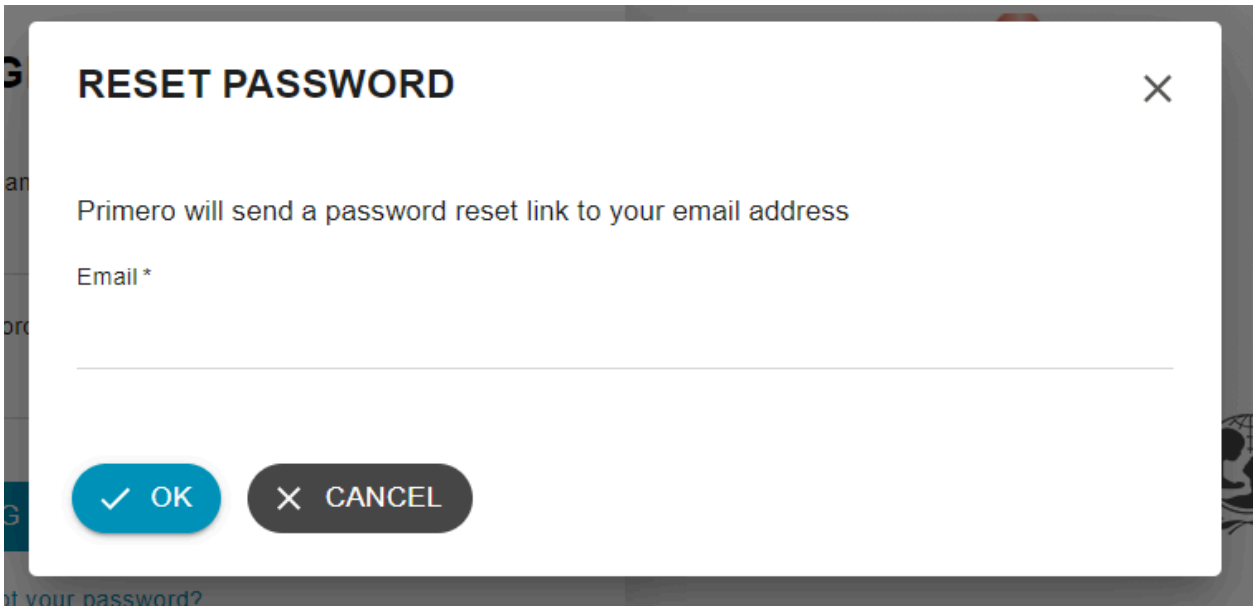
- **Send password reset email:** Go to the User list and click on the User whose password you would like to reset. At the top of the screen, in the **Actions** menu, click the **Send password reset email**. The user will receive an email containing a link which they can use to reset their password.



In addition, Users can always reset their password by clicking the **Forgot your password?** link at the bottom of the Login page.



The User will see a modal where they can enter the email address associated with their User account. They will then receive an email containing a link they can use to reset their password.

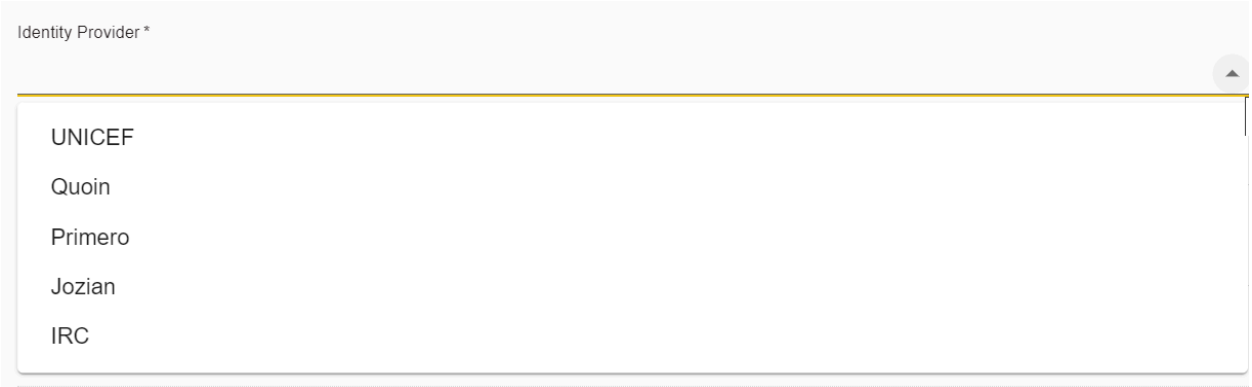


Note: Because Primero often uses password reset emails to help Users set their password, it is *extremely important* that administrators specify an email address for User accounts whenever possible.

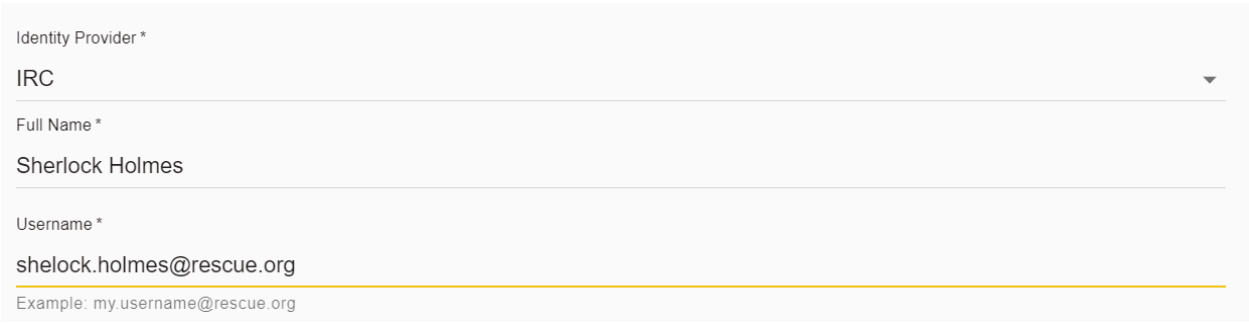
Managing Identity Providers

Some implementations in Primero v2 will use identity providers to manage User accounts (i.e. Users can login using their organizational credentials, such as a UNICEF or IRC username / email address). In implementations configured to use identity providers, creating and updating user accounts will work slightly differently.

- When creating a user account, you must first specify a provider.



- Based on the provider you have selected, you will need to enter a username which matches that provider's username format. For instance, in this example, I have accepted "IRC" as the User's identity provider. Therefore, I must enter a username that ends in "@rescue.org".



- Once you create this User account, the user will receive a welcome email like the one below, telling them how to login.

Welcome to integration-id.primerodev.org!

You have been added as a CP Case Worker.

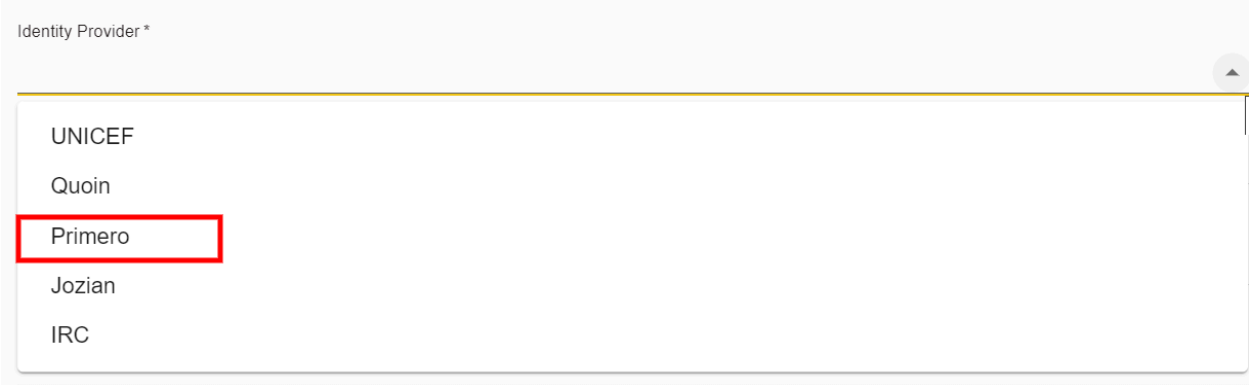
1. Go to https://integration-id.primerodev.org/ and click IRC.
2. Login with your IRC account shelock.holmes@rescue.org.
3. Use the same password you always use for your IRC account.

Please contact Jack Miszencin (miszenci@quoininc.com) for further details.

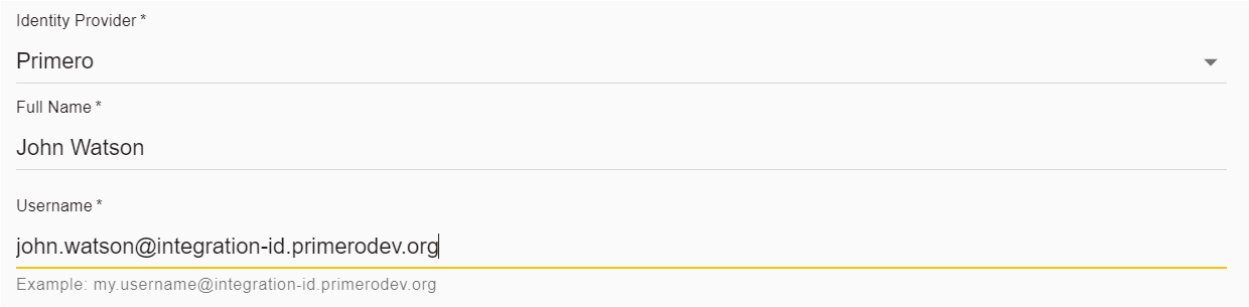
- ***Note**: Primero administrators do not manage passwords for users who login with an identity provider account. All password management is performed by the identity provider.*

Organizations Without Identity Providers

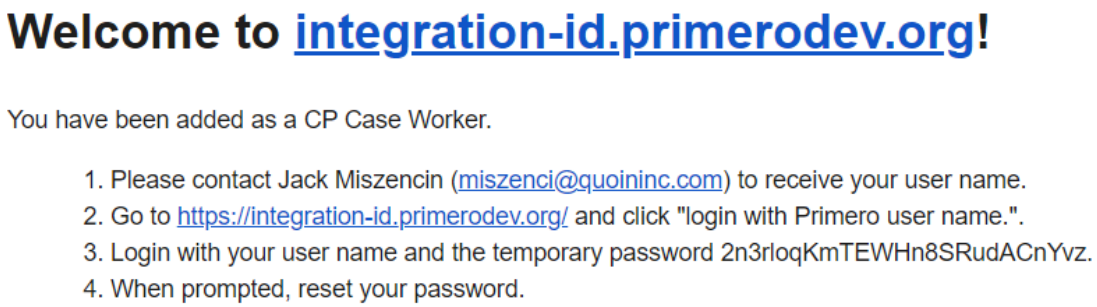
In some systems which have been configured to use identity providers, there will still be some organizations who do not use an identity provider. To create User accounts for these organizations, use the “Primero” identity provider.



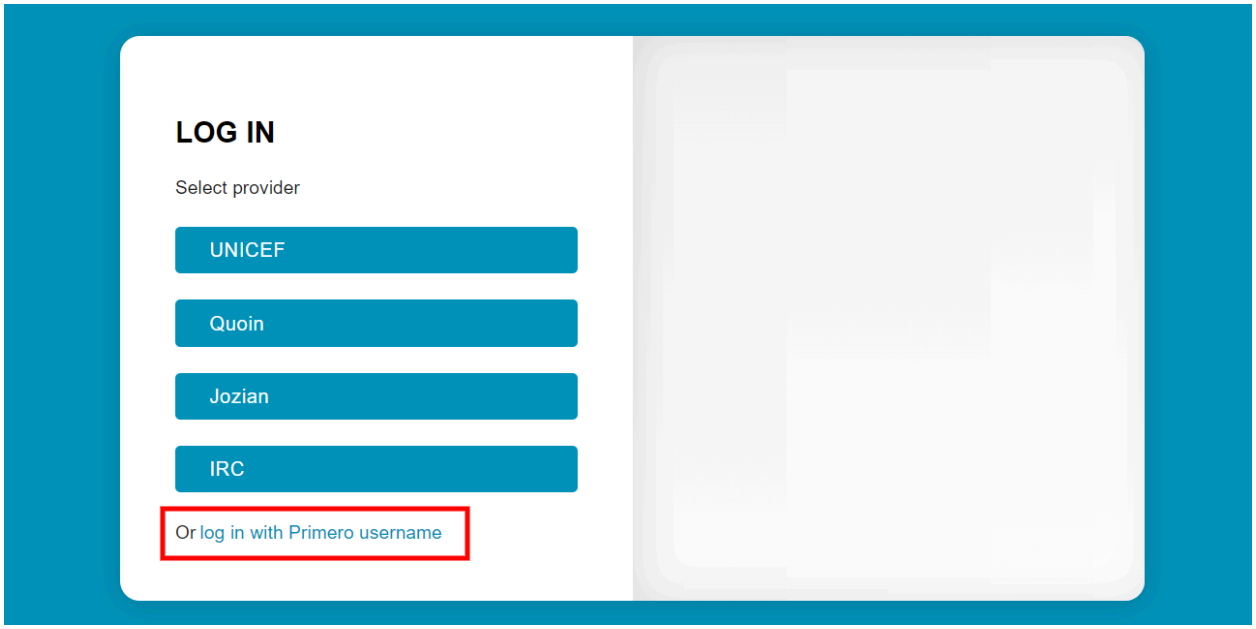
Once you have selected the “Primero” provider, you will enter a username which ends in the Primero site’s URL.



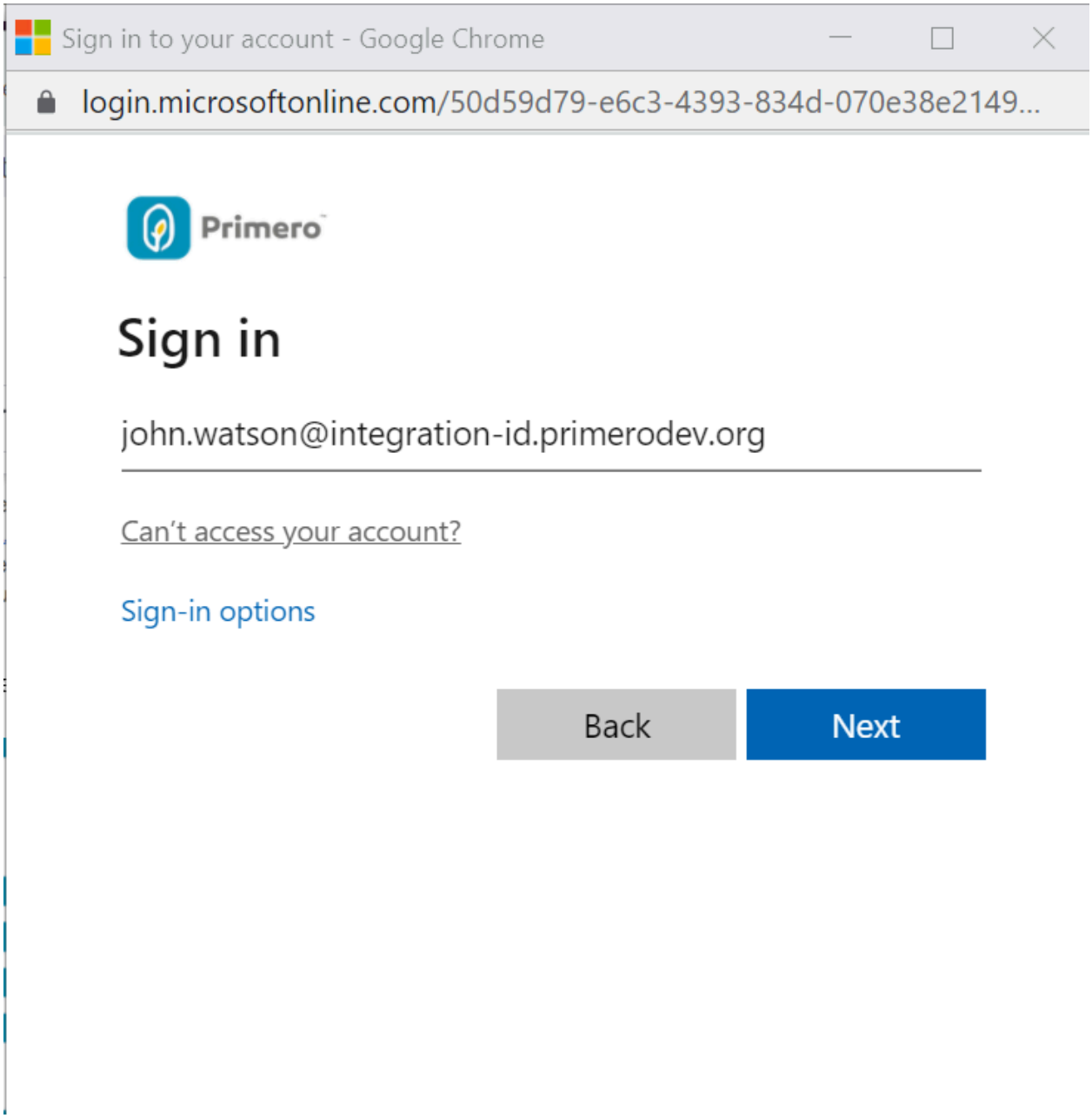
When you create this User account, the User will receive a welcome email containing a temporary password. ***Note:*** *At this point, you as the administrator will be responsible for sending the user their Primero username so that they can login.*

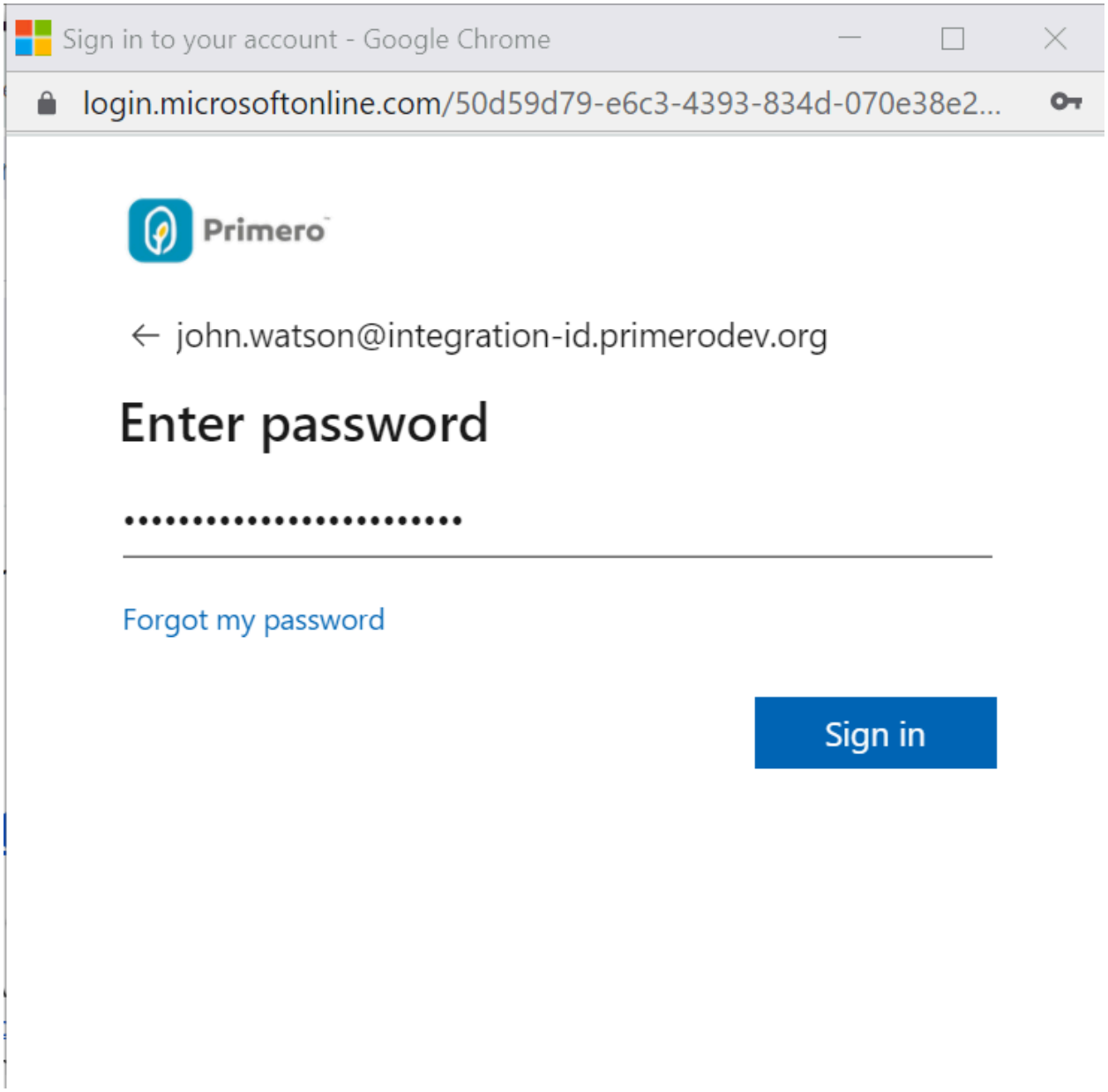


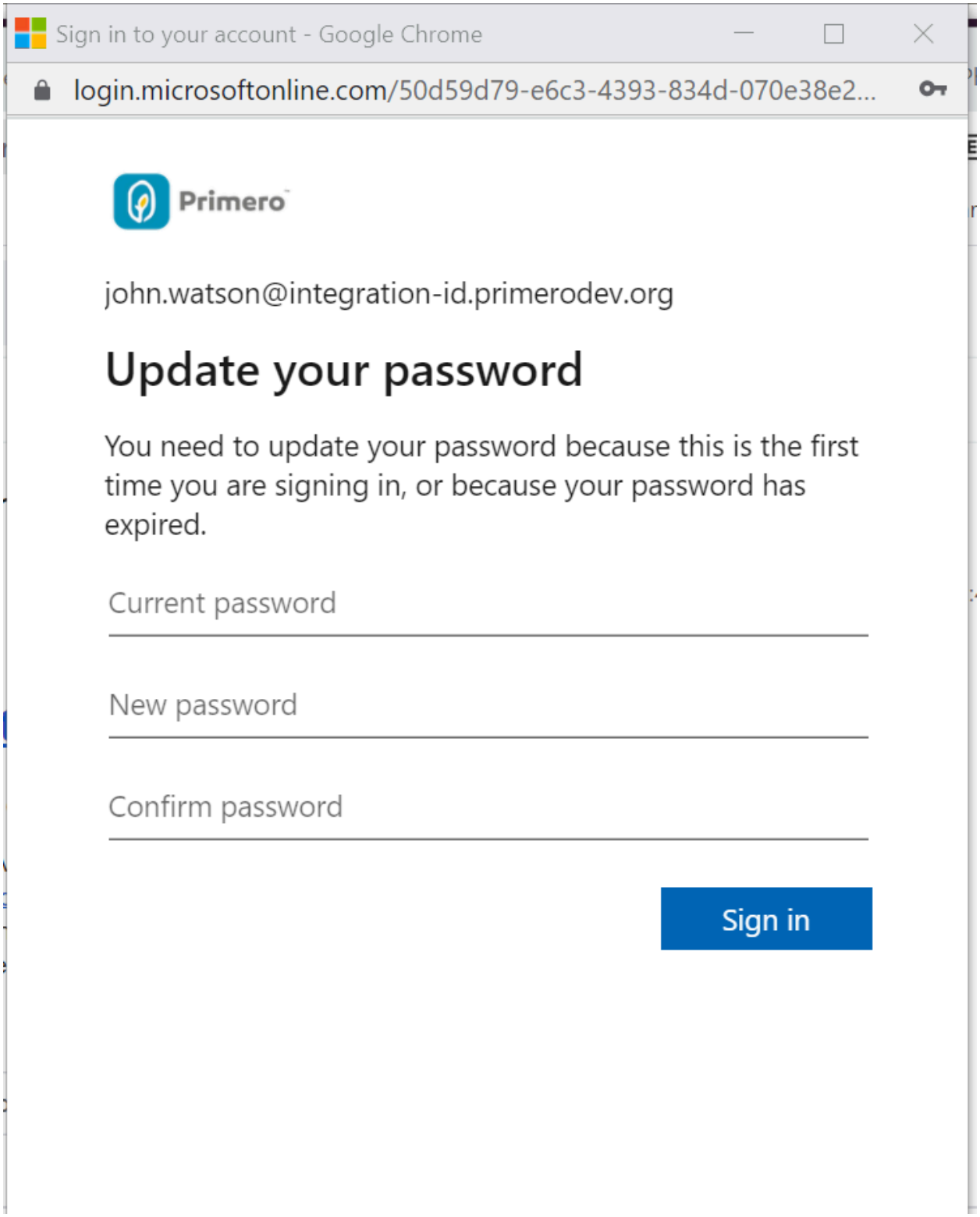
If the User clicks on the link in the email, they arrive at the Login page, where they click **Login with Primero username**.



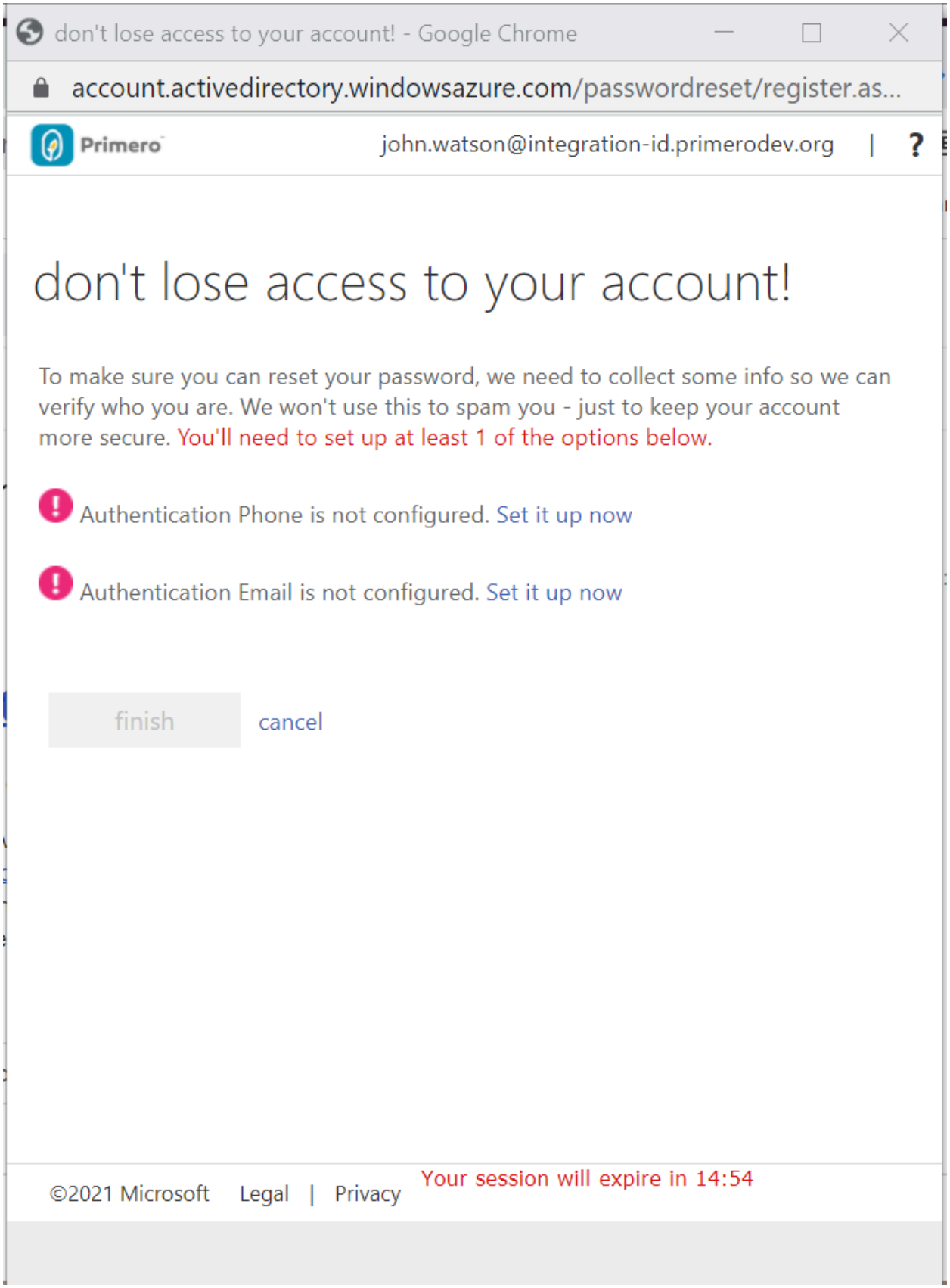
At this point, a separate window will open where the User will be prompted to enter their Primero username, then their temporary password.


Sign in to your account - Google Chrome
login.microsoftonline.com/50d59d79-e6c3-4393-834d-070e38e2149...
Primero
Sign in
john.watson@integration-id.primerodev.org
Can't access your account?
Sign-in options
Back
Next

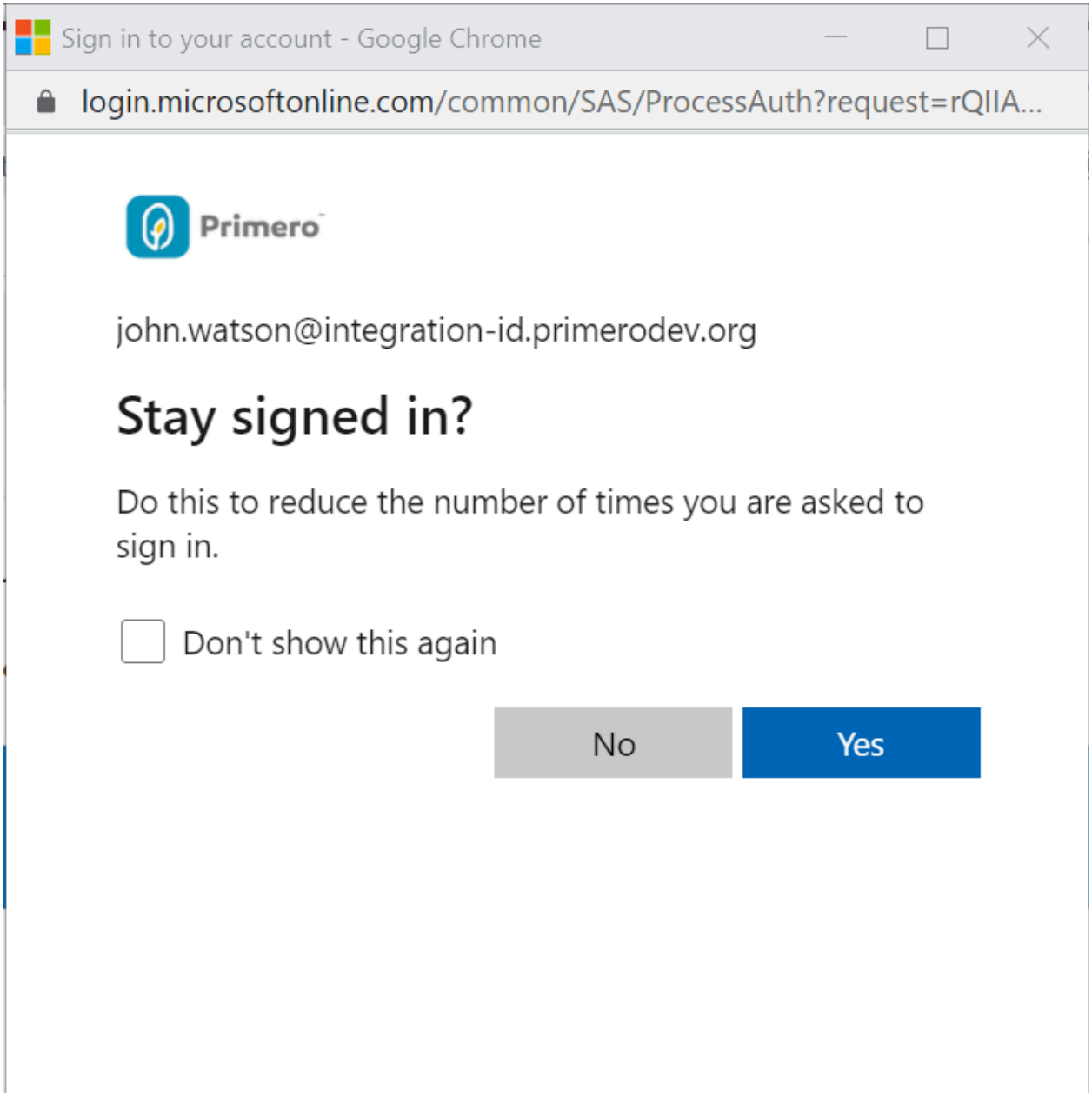

Sign in to your account - Google Chrome
login.microsoftonline.com/50d59d79-e6c3-4393-834d-070e38e2...
Primero
← john.watson@integration-id.primerodev.org
Enter password
••••••••••••••••••••••••
Forgot my password
Sign in



Note that, once the User resets their password and signs in, they will be prompted to set up and verify a recovery email address and phone number. This is important, to ensure that Users have a way of recovering their account should they lose access.


don't lose access to your account! - Google Chrome
account.activedirectory.windowsazure.com/passwordreset/register.as...
Primero
john.watson@integration-id.primerodev.org
don't lose access to your account!
To make sure you can reset your password, we need to collect some info so we can verify who you are. We won't use this to spam you - just to keep your account more secure. You'll need to set up at least 1 of the options below.
Authentication Phone is not configured. Set it up now
Authentication Email is not configured. Set it up now
finish
cancel
©2021 Microsoft
Legal
Privacy
Your session will expire in 14:54

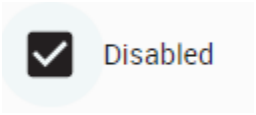
The User may also be asked if they would like to “stay signed in.” For security reasons, it is not recommended that Users do so.



From this point forward, all password management and resets will be handled through the Primero identity provider interface accessed through the Login page. **In order to update the password for users using the Primero Identity, please go to https://aka.ms/sspr.**

Disabling Users

Please note that Users cannot be deleted. Instead, administrators can “disable” a User account by editing the User, then checking the “**Disabled**” tick box. Disabling a username will prevent that username from being used to log in to Primero.



Other Settings

Managing Workflow Statuses for CPIMS+

The below table outlines which fields set each Case Workflow Status:

Workflow Status	**How to set this status (Trigger field)**	**Trigger field ID**	**Developer settings**	**NOTES**
New	[Set by default on case creation]			
Assessment	Fill out the **Assessment Start Date** field.	assessment_requested_on	Only appears as a workflow status if the module has the "**use_workflow_assessment**" attribute set to true. This attribute defaults to false, so if you do not set this attribute, this workflow status will not appear by default.	
Case Plan	Fill out the **Case Plan Initiated** field**.**	date_case_plan	Only appears as a workflow status if the module has the "**use_workflow_case_plan**" attribute set to true. This attribute defaults to false,	

			so if you do not set this attribute, this workflow status will not appear by default.	
Response Type 1, Response Type 2, etc.	Service created with a **Response Type** value of Response Type 1, Response Type 2, etc.	service_response_type	Options are set in the **Service Response Type** lookup. If all service provisions fall under the same step in your workflow, we suggest changing the Service Response Type lookup to have a single option, labelled "Service Implementation", and set this to be the default value for the "service_response_type" field.	Each of these is intended to represent a different category of service provision, which represents a different stage of case management.
Services Implemented	All services are implemented (Service Implemented field has value "implemented"). User sets a service as implemented by filling out the **Service Implemented On** field.	service_implemented_day_time	Only appears as a workflow status if the module has the "**use_workflow_service_implemented**" attribute set to true. This attribute defaults to true, so if you do not set this attribute, the status will show automatically.	

Closed	Set **Case Status** to "Closed"	child_status		
Reopened	Perform **Reopen** action	case_status_reopened		

Managing Configurations

As you make configuration changes, you can save your settings in a **Configuration**. This acts as a snapshot of all your configuration settings at a point in time. Later, when you have made other configuration changes, if you want to undo them, you can find your saved **Configuration** and *apply* it to return your system to how things were configured at that point in time.

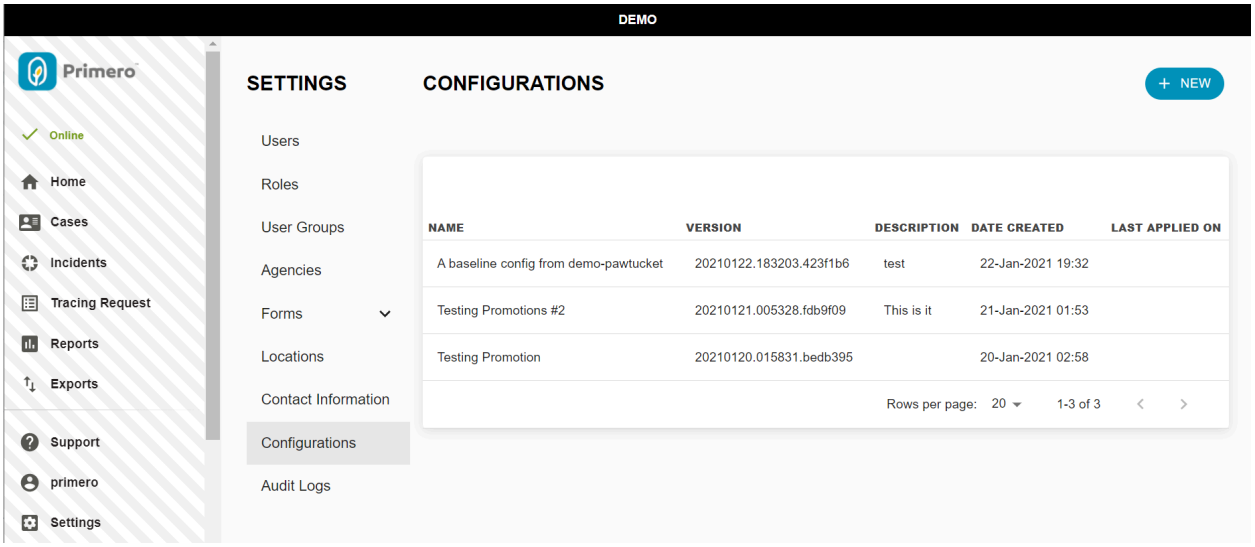
What do configurations include?

- Roles
- User Groups
- Agencies
- Forms
- Lookups
- Reports

What do configurations NOT include?

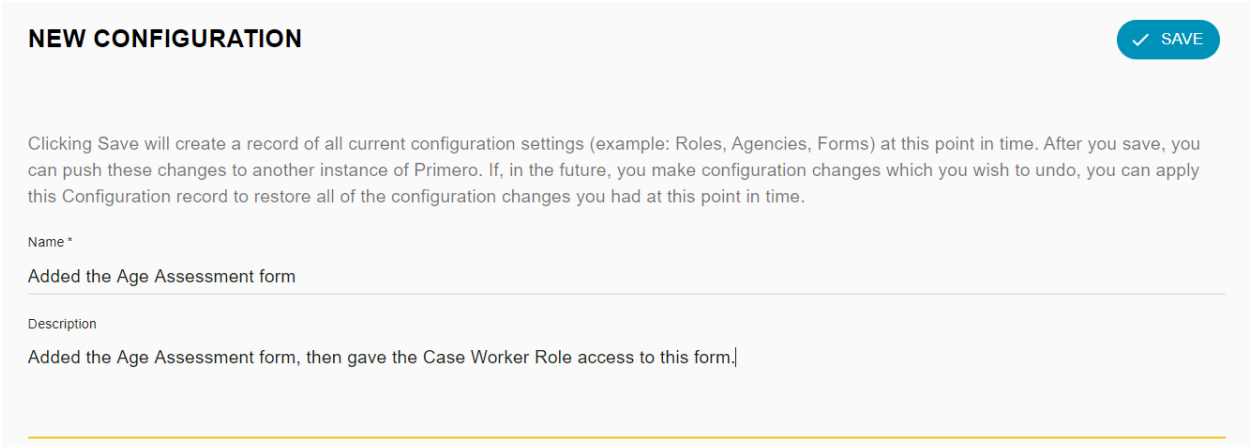
- Cases
- Incidents
- Tracing Requests
- Locations
- Contact Information
- Users
- *Note: User Groups can also be added directly into production*

To view all your saved Configurations, click the **Settings** link in the navigation menu, then click the **Configurations** link in the Settings navigation menu. You will arrive at the Configurations List page.



Creating Configurations

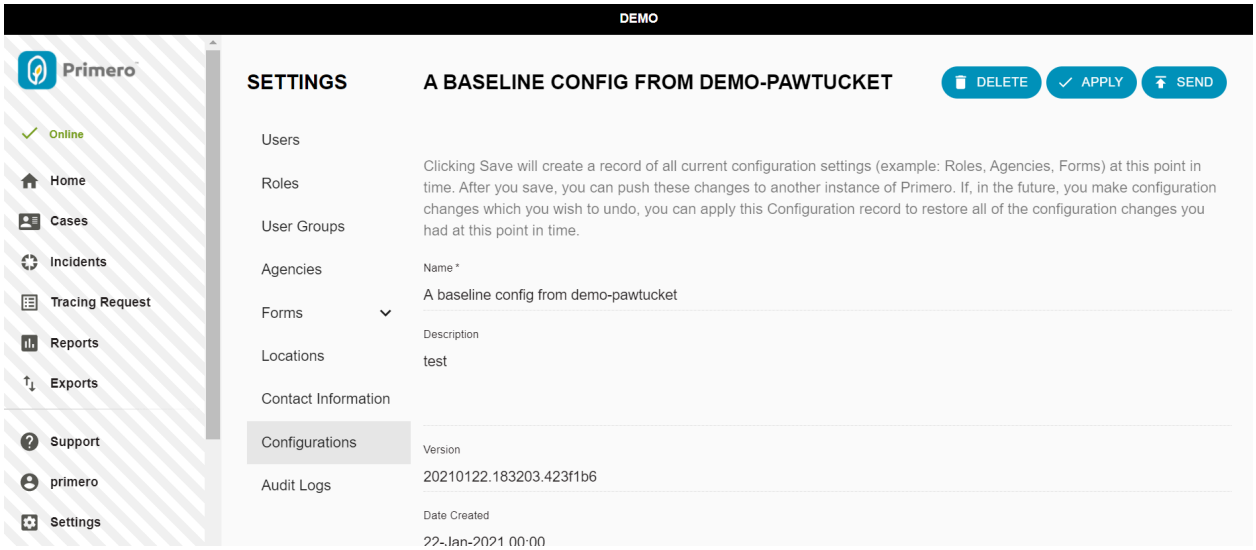
To create a new Configuration, click the **New** button at the top of the page.



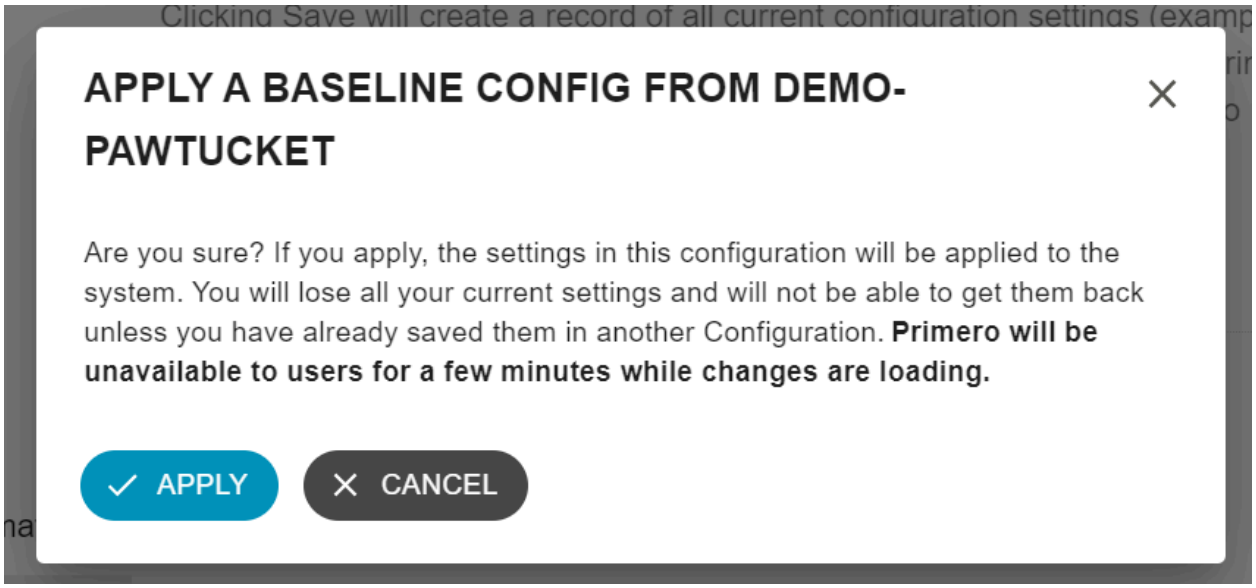
Enter a Name and Description, then click **Save**.

Applying Configurations

To apply a Configuration you had previously created, click into the Configuration in the Configurations list. You will see information on the Configuration, including when it was created, who created it, and when it was last applied.



Click the **Apply** button at the top of the page. The site will be unavailable momentarily to *all users* while the Configuration is applying. For this reason, it is important to only apply Configurations during periods of low site usage.



Once your Configuration has applied, Users should experience the system configuration as it existed when the Configuration was first created.

Note: *You will not be able to apply a Configuration which was created on a higher version of Primero than the one you are using. For instance, if you create a Configuration on your sandbox site, which is running Primero v2.1.1, then send that Configuration to your production site, which is running Primero v2.1.0, you will not be able to apply the Configuration on production until the production site is also upgraded to v2.1.1.*

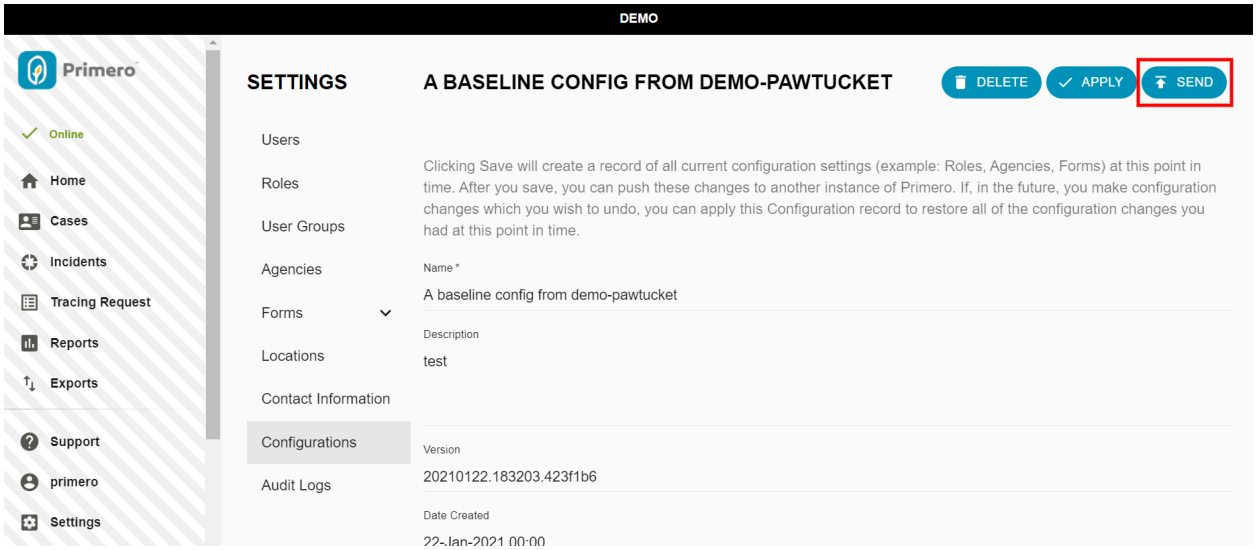
Note: *Applying a past Configuration will not delete configuration records such as Agencies and User Groups which were created after that Configuration was saved. Instead, these will be disabled, which will limit their visibility in the system. For instance, suppose you save a Configuration titled "Added Agency A" on March 1, then create Agency B on March 2. If, on March 3, you apply the "Added Agency A" Configuration, Agency B will still exist in your system but will be disabled. This will mean that any Users assigned to Agency B on March 2 will still exist and function normally, but administrators will no longer be able to assign new Users to Agency B.*

Sending Configurations to Production

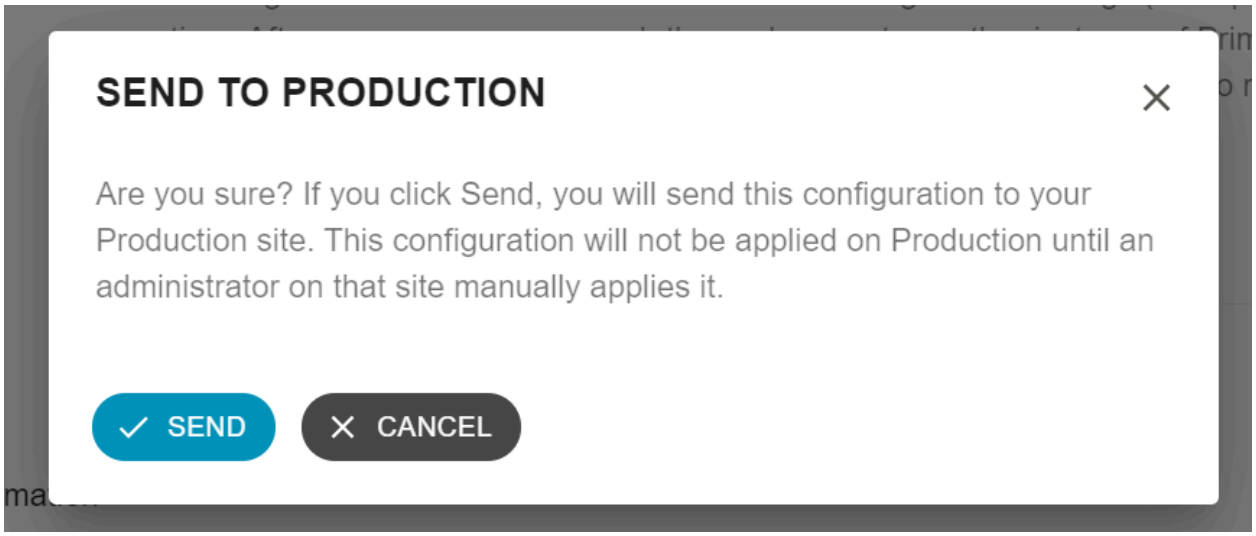
As mentioned in the **Where to Make Configuration Changes** section, it is recommended that you make configuration changes on a sandbox or "demo" site, test them, then send them to your production site to be applied. This translates into the below steps:

- Make configuration changes on your sandbox site.
- Save a Configuration with your changes on the sandbox site.
- Test your changes on the sandbox site.
- Once you have tested your changes, *send* your Configuration to the production site.
- At a time of low production site usage, *apply* your Configuration on the production site.
- ***Note****: You should always communicate your plans to apply a Configuration on the production site with implementation partners.*

To send a configuration from your sandbox site to your production site, go to the Configurations list on your sandbox site. Click into the Configuration you want to send. Click the **Send** button at the top of the page.



You will see a confirmation message warning you that the Configuration will need to be manually applied on the production site. Click **Send** again.



Login to your production site and go to the Configurations list. Find the Configuration you just sent from the sandbox site and click it. Click the **Apply** button to apply the Configuration to your production site.

Limits on Configuration Management in Production

Note that, since you will be making most of your configuration changes on the sandbox or “demo” site, you will not be able to make some configuration changes on the production site except by applying a saved Configuration. This means you will not be able to create or update the following resources on the production site:

- Forms

    - *Note that this includes updates to fields and translations.*
- Lookups
- Agencies
- Roles

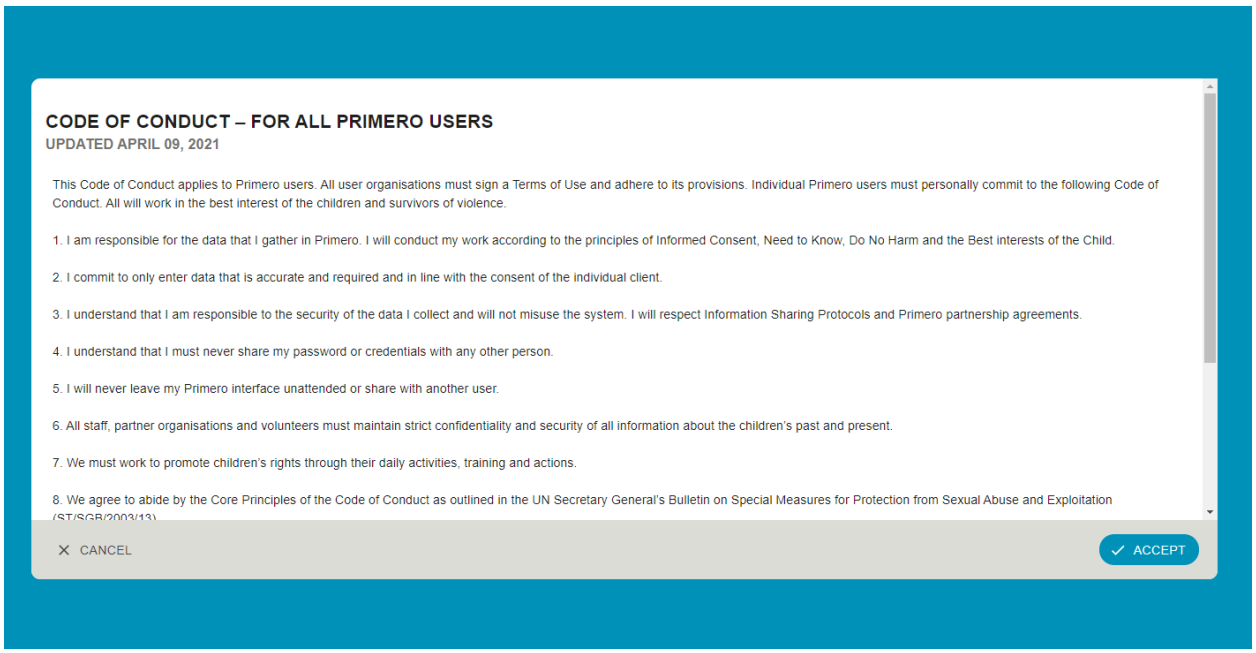
You will still be able to make changes to the following resources on production:

- Reports
- User groups
- Users
- Contact Information
- Locations

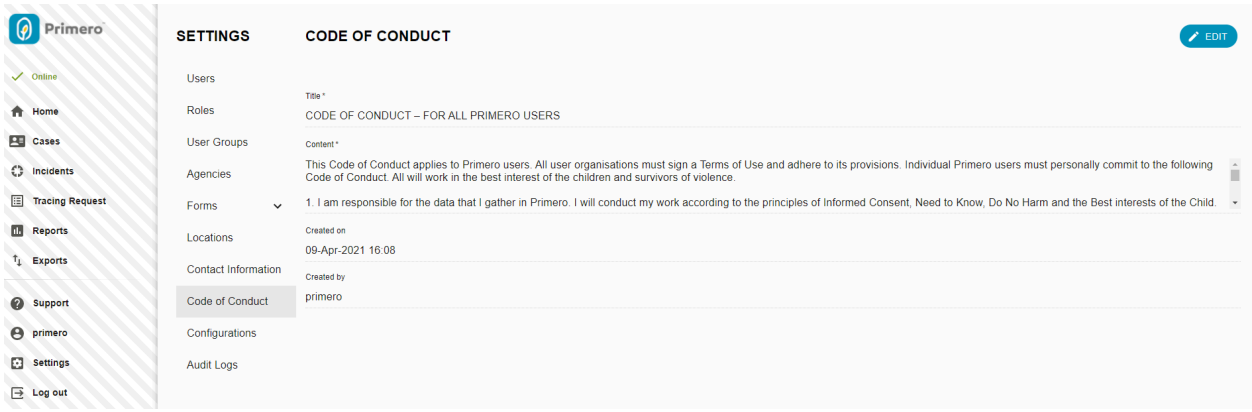
Note: the configuration changes made to production directly do not need to be saved in production. The reports, user groups, users, contact information and locations will remain in production.

Code of Conduct

When initially logging onto Primero, users will be prompted to review and accept a code of conduct:



The code of conduct is editable through the “Settings” under “Code of Configuration”. Administrators can modify the terms of the code of conduct as defined by the programme.



Error Messages in Primero

In order to support you when you receive a specific error message on your browser when you are using Primero, please follow the below guidance:

Are you seeing this error message?	**What does it mean?**	**What do you do?**
A popup indicating you need to either log back in or press continue.	The session has been inactive and this pop up appears after 5 minutes of idle time.	You can either log back in or press continue to resume with the session.
error: [missing "en.forms.record_types.undefined" translation]	There is a translation that is missing when you are trying to make a request.	Send a screenshot to the Primero System Administrators skype chat and describe the process of what you were trying to do so the team can debug the issue.

errors.api.internal_server	This is a generic error given when the server cannot process something you are requesting.	Wait a few minutes and try again. If the error continues, watch this video and send a message to the Primero System Administrators skype chat or the Primero Support Hub informing the team. Please include your country/URL, what day and time when you saw this error and describe the process of what you were trying to do so the team can debug the issue.
Unexpected token “<,” ‘<html> <h” … is not valid JSON	This is an issue in the JSON code and needs to be fixed by the developers.	Watch this video and send a screenshot of the error to the Primero System Administrators skype chat or the Primero Support Hub informing the team. Please include your country/URL, what day and time when you saw this error and describe the process of what you were trying to do so the team can debug the issue.

errors.api.internal_server failed to fetch	This is a network error given when the server cannot process something you are requesting.	Do you see your logo in the bottom left corner of the navigation? If not, please reload your screen. If you still see the error, please log out and log in again. Were you attaching a file? If yes, are your attachments successfully attached? If not, log out and log back in again. If the error continues, watch this video and send a message to the Primero System Administrators skype chat or the Primero Support Hub informing the team. Please include your country/URL, what day and time when you saw this error and describe the process of what you were trying to do so the team can debug the issue.
400 Bad Request	The server cannot process the request due to an error from the user or the user's device.	Try the following options in the order below: 1. Double check the website address. 2. Refresh. 3. Log out and log back in. 2. If that does not work, clear your browser's cache or cookies.

		3. Send a message to the Primero System Administrators skype chat to help debug.
403 Forbidden	You do not have access to a specific functionality within Primero.	Reach out to the Primero team on the functionality you were trying to access and they will be able to provide you with further guidance. Please provide us with the role that got the forbidden error, the website/URL and please describe what you were trying to do (for example, trying to save a case, add a user, etc.).
500 Internal Server Error	This is a generic error given when the server cannot process something you are requesting.	Send a screenshot to the Primero System Administrators skype chat. Please include your country/URL, what day and time when you saw this error and describe the process of what you were trying to do so the team can debug the issue.
502 Bad Gateway – Microsoft Azure Application Gateway	The server is not available and the infrastructure team needs to get the system back up.	Wait a few minutes and try again. If the error continues, send a message to the Primero System Administrators skype chat or the Primero Support Hub informing the team. Please include your country/URL,

		what day and time when you saw this error and describe the process of what you were trying to do so the team can debug the issue.
504 Gateway Timeout	This error indicates an issue with your network connection or server communication speed.	Wait a few minutes and try again. Refresh your screen. If the error continues, send a message to the Primero System Administrators skype chat or the Primero Support Hub informing the team of the day and time when you saw this error and describe the process of what you were trying to do so the team can debug the issue.
This site can’t be reached	This error indicates an issue with your network connection or server communication speed.	Try the following options in the order below: 1. Check connectivity 2. Refresh your page. 3. If that does not work, try “Incognito mode”. 4. If that does not work, try a different browser. 5. If that does not work, try with different devices. 6. Send a message to the Primero System Administrators skype chat to help debug.

Syncing data: not able to see data that has been saved (including attachments)	The user saves a case or uploads a document and presses save. The data isn't appearing when logged in as a supervisor, or the user is not able to see their downloads.	1. Check the change log to see if the updates were saved to the case 2. If the data is in the change log, check if you are in "online" mode 3. If you are in "online" mode, inform the Primero team of the user name and time when the error occurred. 4. The Primero team may also ask you to take a screenshot of "Network" and "Error" tabs in your Inspect console to help troubleshoot.

Primero Reporting using Power BI and the Cases API

Purpose: This is a step-by-step guide for pulling case data from Primero Cases API into Power BI for data visualization.

1. **Make sure you understand what an API is and how it works.** An API is a way for two digital systems to securely communicate and share data. In Primero, the API works like any other user, based on the permission of that user's role. It allows raw data to be shared digitally without having to extract it (via export) from Primero. APIs can do different things, but for our purposes we are going to use the "GET" data and "POST" data requests. Read more here.
2. **Check to make sure you have access to cases in your Primero instance.** Only users with existing access to case records will have permissions on the Cases API. Any user can access the API endpoint for something they would normally

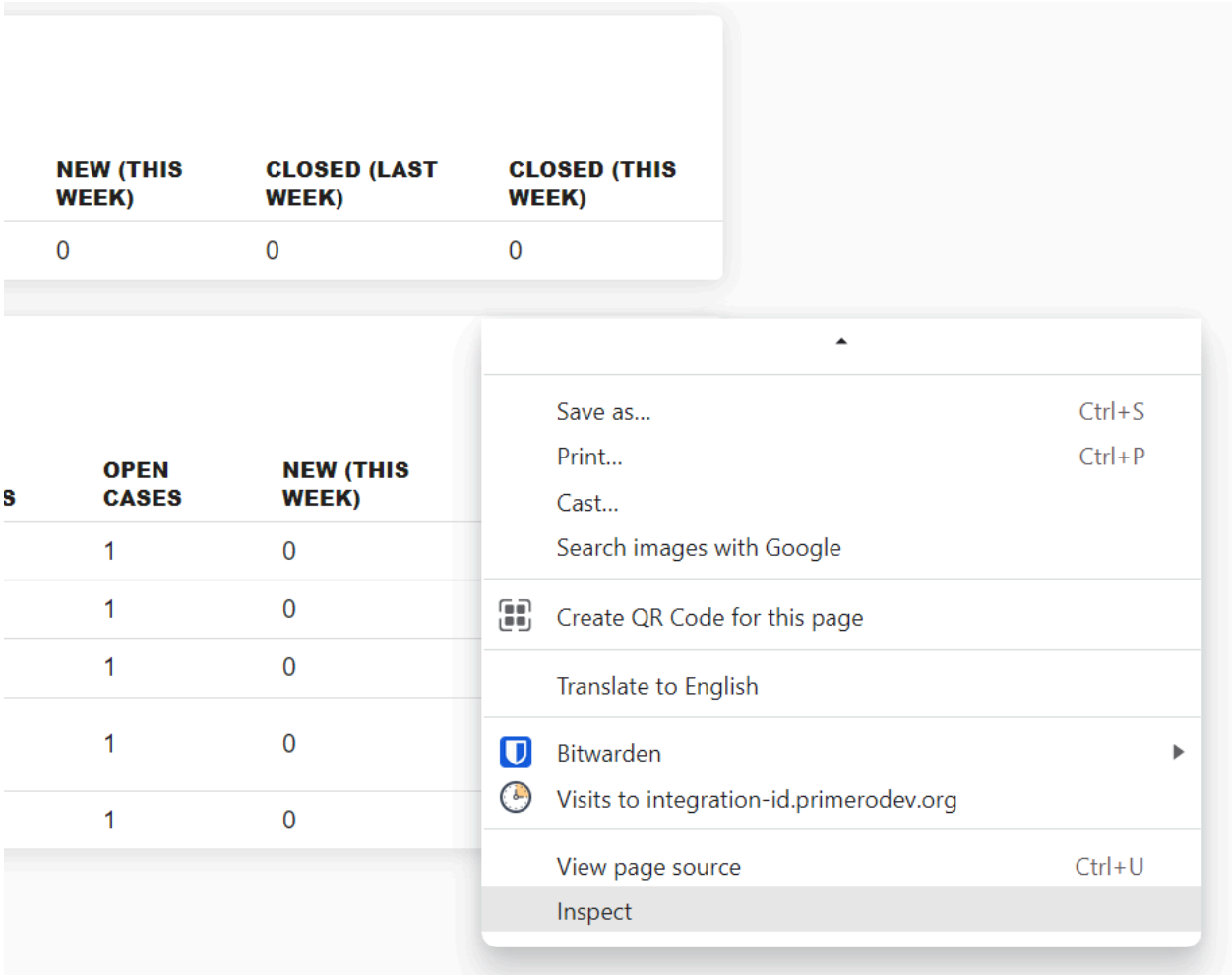
access in the UI. If you can see the case list in the Primero UI, you can also access the Cases API. If you can access users in the Primero UI, you can also make requests to the Users API. For the purposes of doing powerbi analysis on cases, a user would need to have view access to cases (edit access not necessary). To limit the access a user has to specific information about cases in the API, you would update which case forms their role has access to.

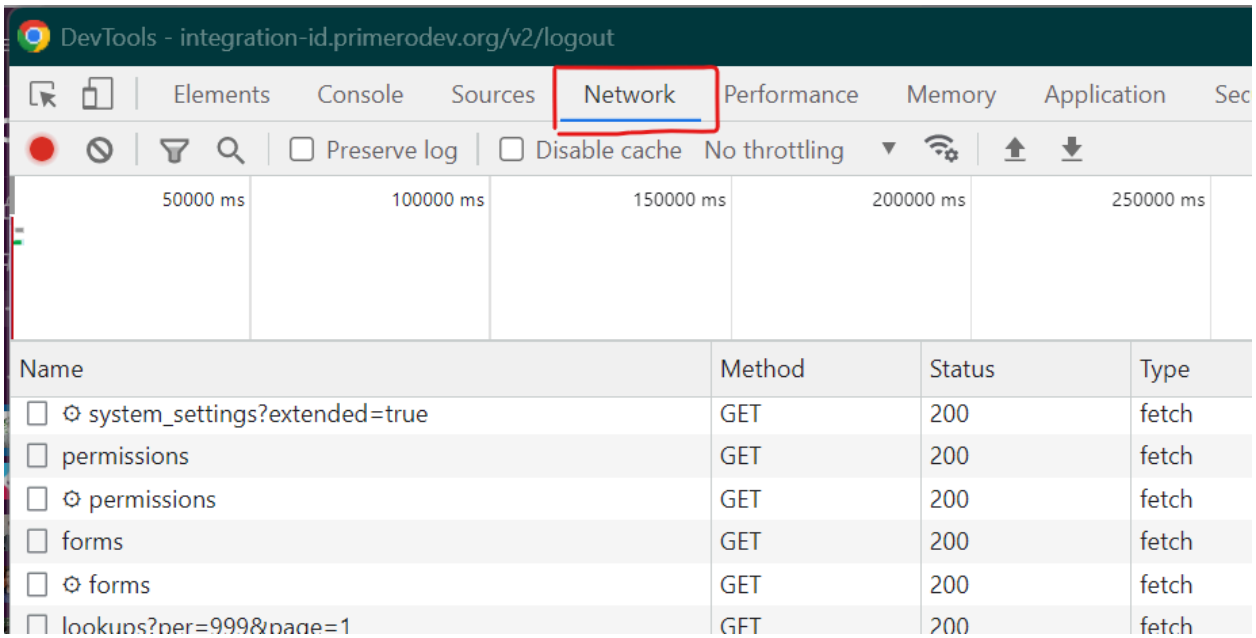
3. **Always consider data privacy and data protection first**. Access to case data should always be confidential. If you intend to access the Cases API, this access should be approved by the relevant authorities and be in-line with your information sharing protocols and regulations. If you are creating a new role for reporting using the API, make sure that this role is designed, tested and approved by the relevant authorities. *DATA PROTECTION IS YOUR RESPONSIBILITY.*
4. **Do a little research on Power BI.** What is it? What can it do? What type of needs do you have? What type of account do you have? Learn about visualizations, dashboards, reports, apps, and datasets (Power BI content) and workspaces.You can find lots of relevant information and videos online. Start here
5. **Think about the data you want to use in Power BI.** It's important to think ahead about what you want to do. You need to have a **clear purpose** for your use of the data. What relationship(s) do you want to show? Think this through before you set up your API call.
6. **Make sure you understand how the API parameters work.** To make sure you are getting the right information from the API, it is important to understand how to use an API endpoint's URL parameters. Take the time to learn about these before getting started.
    - Here is a quick guide on how to format URL parameters: https://apipheny.io/what-are-api-parameters/
    - Here is the documentation for the Cases API: https://github.com/primeroIMS/primero/blob/master/doc/api/cases/get.md
    - Note that the Incidents and Tracing Requests API endpoints will have approximately the same guidelines as those laid out in the documentation for the Cases API. The endpoints for these are:
        - Incidents: /api/v2/incidents
        - Tracing Requests: /api/v2/tracing_requests

7. **Prepare to make your API call**. Every time you have PowerBI pull information from the Cases endpoint, you will need to enter a URL. When asked to pick an authentication, choose “Basic auth,” and enter your username and password.

    a) If your implementation uses single sign-on, you will need to use a different authentication method.

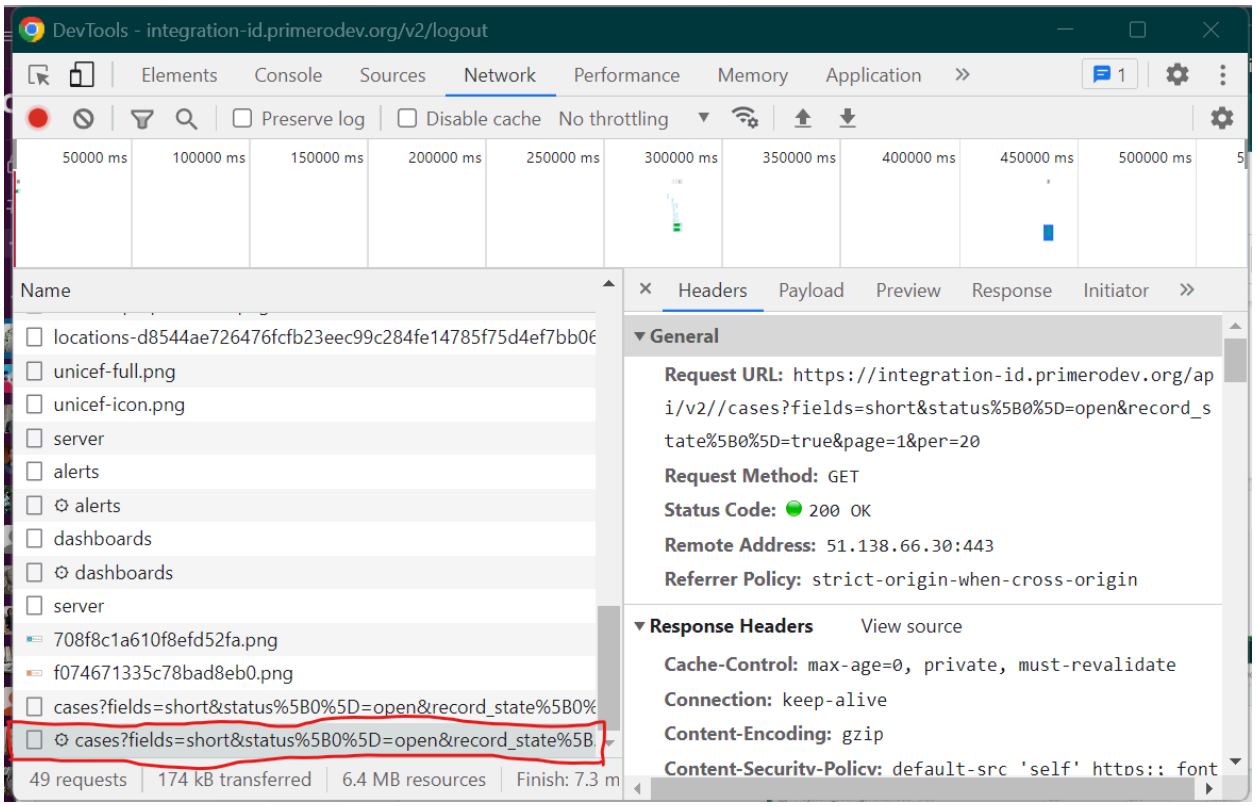
        1. First, in your browser, go to Primero and sign in.
        2. Next, open your browser’s developer tools. In Chrome, you right-click anywhere on the page and click “Inspect.” Then click into the “Network” tab.



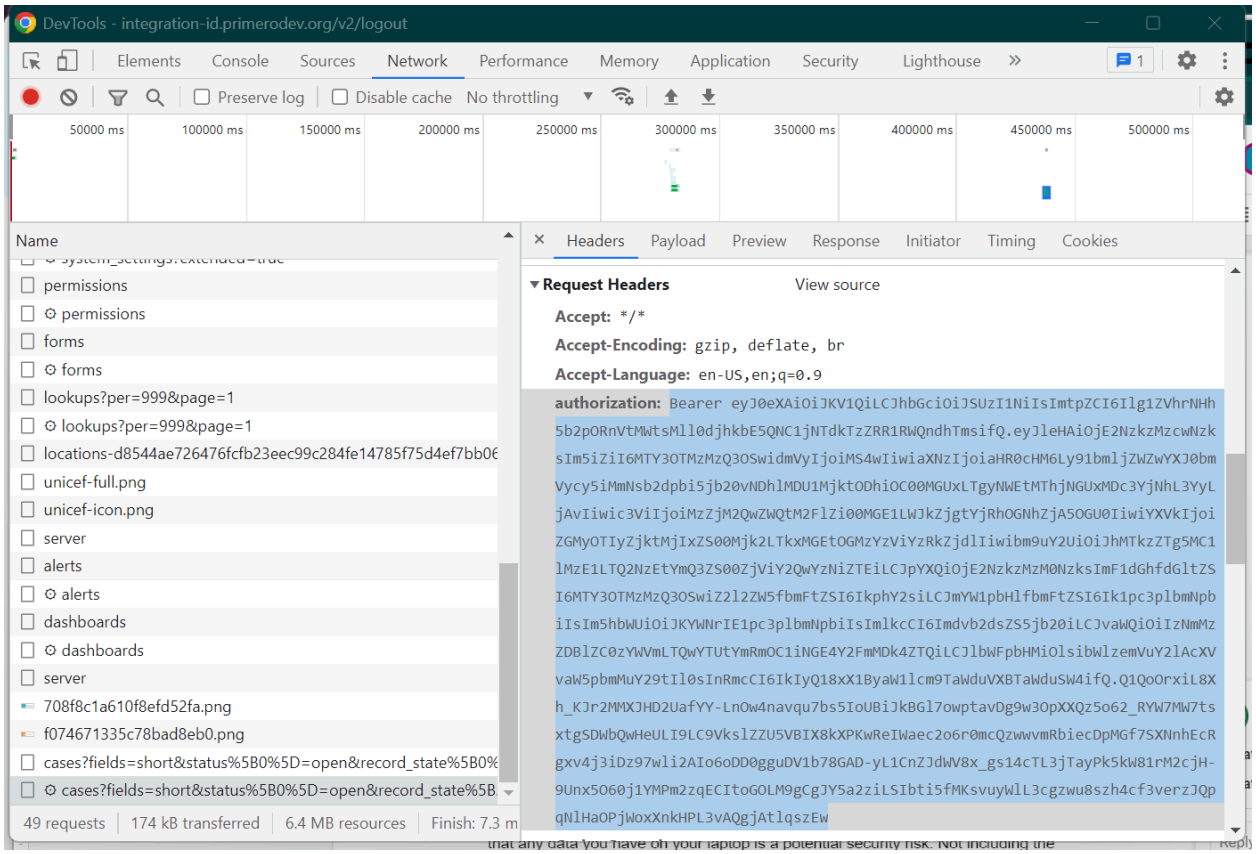


3. Now, in Primero, click on the Cases list.

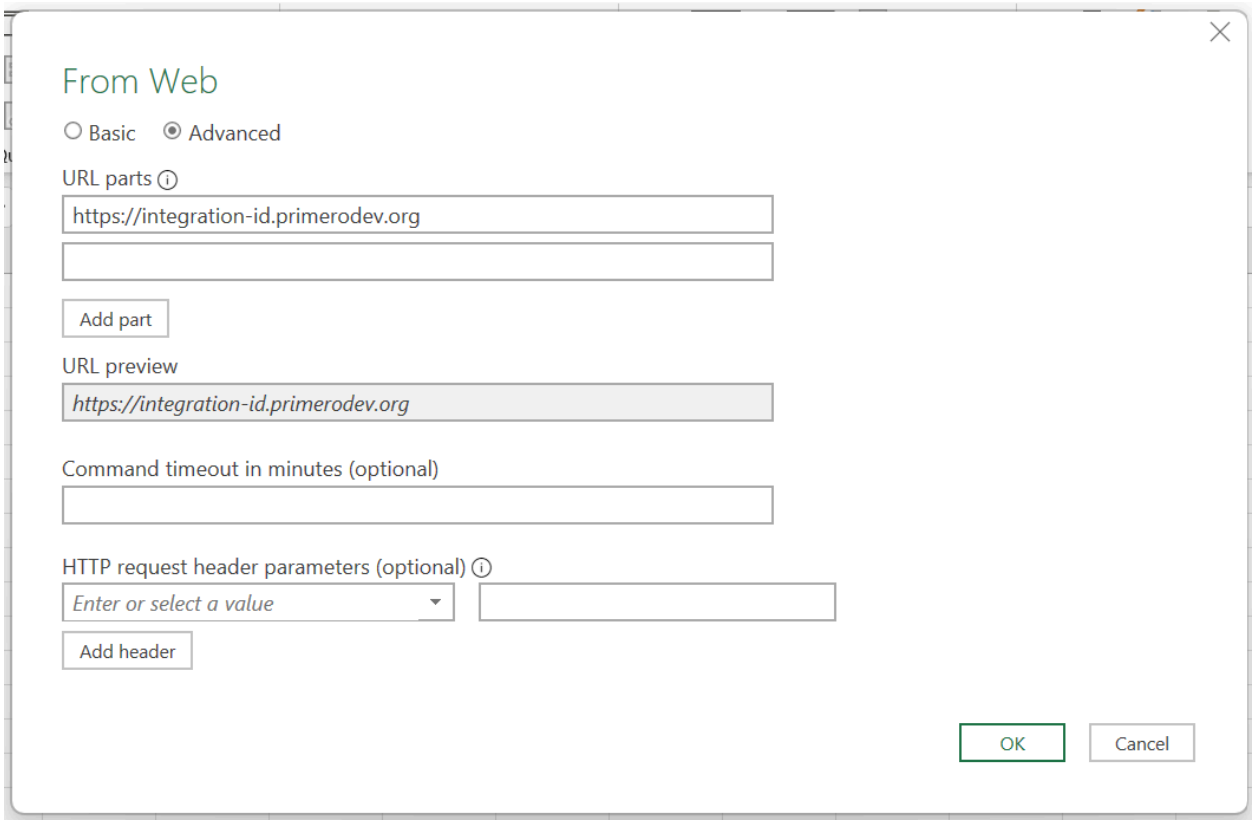
4. In the “Dev tools” window, in the Network tab, click on the most recent request in the list.



5. When you do this, details of the request will appear on the right. In this pane, scroll down until you reach the section labeled “Request Headers.” Find the header called “authorization.” Highlight the whole value of this header, including the word “Bearer.” Copy this.



6. In PowerBI, when you start to pull data from a “Web” source, choose the “Advanced” option in the modal which appears. Under “HTTP request header parameters,” enter “authorization” as the header name, and then paste in the value you copied from your browser developer tools.



7. When you click “OK,” you will be automatically authorized. Note that this authorization header value which you copied will expire roughly once every 30 minutes. If you have trouble connecting to the API after a certain point, try repeating the steps here.

When entering a URL, you may want to add the following parameters:

- **fields:** This tells the API which fields to include in its response. By default, the API will only send back all available fields on the case. Passing in the fields parameter limits the size of the JSON response and only includes the information you need to analyze. This last part is very important for preventing the leaking of sensitive data. Remember that any data you have on your laptop is a potential security risk. Not including the fields parameter can cause the

response to time out, cause PowerBI to crash if the response size is too large, and can lead to you having sensitive information on your laptop.

    - Example: to only include the Protection Concerns and Risk Level fields, you would add the following parameter to your URL: fields=risk_level,protection_concerns

- **per and page**: The first of these two parameters tells the API how many Cases to include in the response, while the second tells the API which page of results you would like to review. Just like when you are viewing the Case list in Primero, if you leave these blank, the API will default to showing 20 results per page and showing you the first page of results. To view a large number of results, you can either set the per parameter to a very large number (e.g. 10000) or do multiple requests to the API, increasing the page parameter every time.
    - Examples:
        - To include 500 results per response, and view the second page of results, add the parameters per=500&page=2.
    - General filtering parameters: You can add in parameters that filter the results based on field values. Note that this gets formatted differently for different types of fields.
    - Example: To only include Cases between the ages of 10 and 15, and with the protection concerns “Unaccompanied” or “Separated, add the parameters sex=male&age=10..15&protection_concerns=unaccompanied,separated

8. **Submit your API call**. PowerBI can pull the JSON response from this API and import it for analysis.

Primero and RapidPro

In order to get RapidPro to create cases within primero, or to edit fields within existing cases in Primero, we need to use the Primero API. RapidPro's Call *Webhook* node type allows us to interact with APIs such as the Primero API in a RapidPro flow.

You only need to do these steps once per integration of RapidPro and Primero.

Accessing the Primero API requires credentials. Generally, it is best practice to create a RapidPro specific user which can only access a minimal set of resources. Once the user has been created, you should take note of its username and password.

As we will be using these credentials over a long period of time, it is most straightforward to use *Basic Auth* to authenticate to our webhook.

In order to generate a *Basic Auth* string, you need to encode the credentials into Base64. If you are using a MacOS or Linux machine, you can do this in a shell with the following command:

```
printf '<username>:<password>' | base64
```

Alternatively, you can use a tool such as Postman or Httpie to try out various API commands (and generate a basic auth string).

Once you have determined what your *Basic Auth* string is, you can save it to a global variable in the relevant RapidPro workspace. It is possible to access the global variables at **/global**

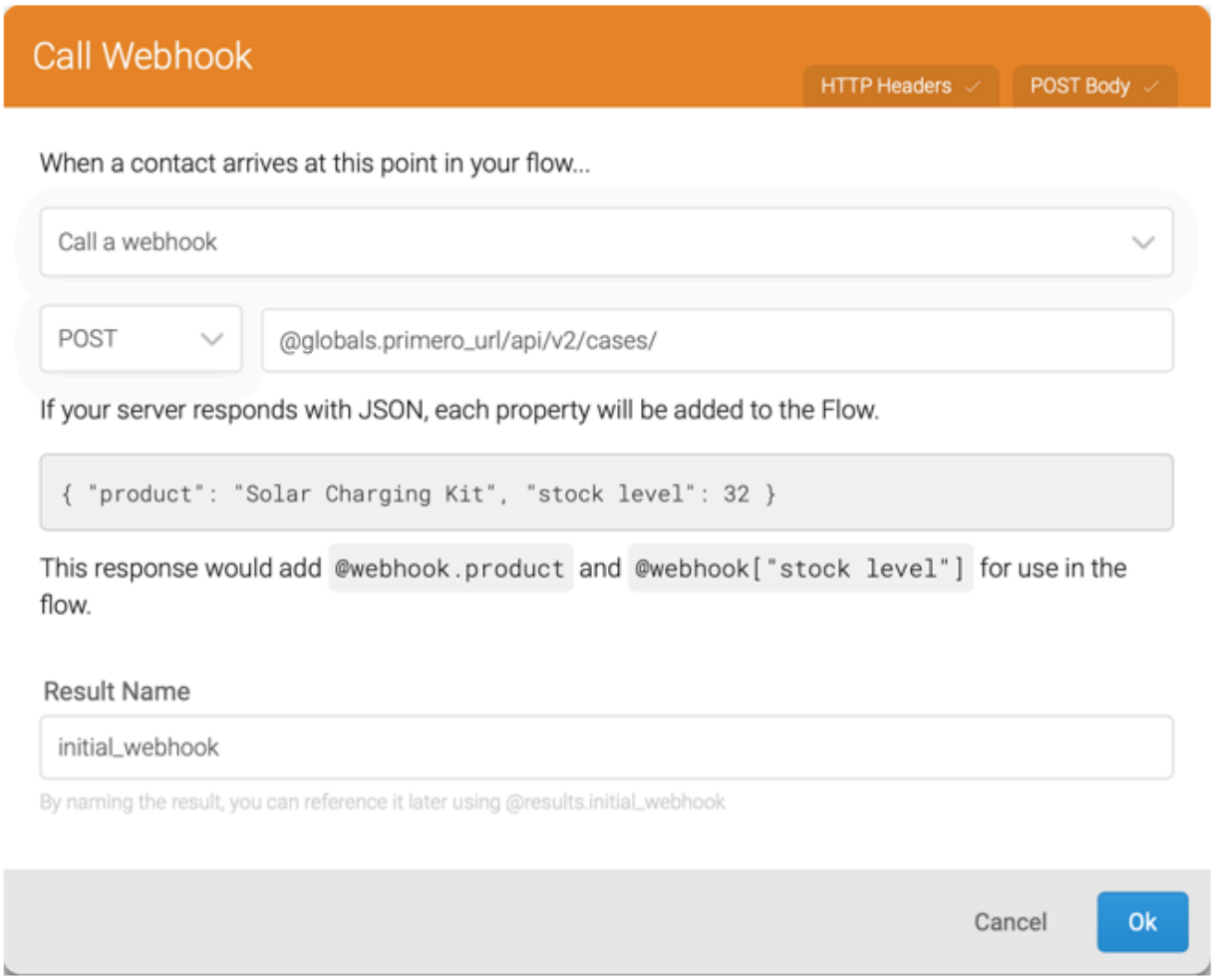
on your rapidpro instance. You should also set the URL of your primero instance to a global variable.

NOTE: All users with permissions on Rapidpro workspace can access this global variable. They can therefore access any resource that the rapidpro user can access on Primero. Only give RapidPro access to trusted users.

Creating cases

The most common thing we are likely to do with rapidpro is to create a case. In order to do that, we first need to create a "*Call Webhook*" node. There are three tabs with configuration details that need to be set.

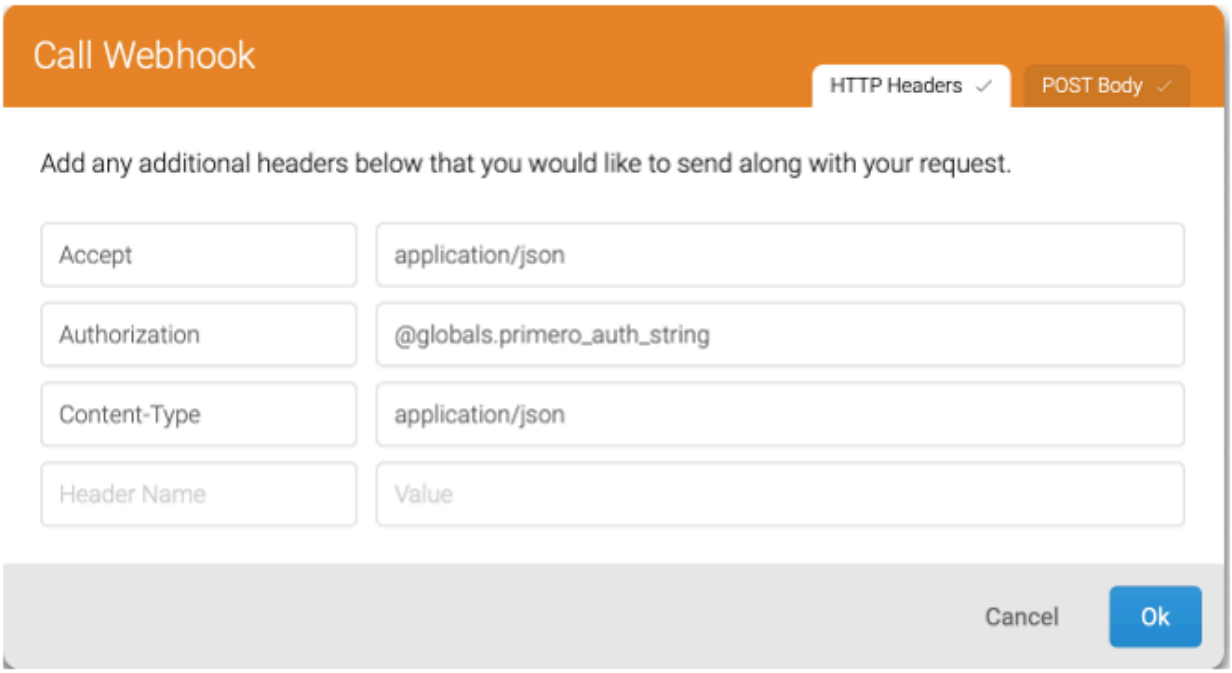
The first tab is the one that opens by default. In this tab, you need to set the HTTP verb to *POST*, and set the URL of the webhook. You will be able to do this by referencing the global variable you created earlier (@globals.primero_url in the screenshot below). After the global variable, you need to set the route, which for cases will be **/api/v2/cases/**. If you wanted to create an incident, it would be **/api/v2/incidents/**



Click on the second tab HTTP headers. Primero expects the following headers:

1. accept
2. authorization
3. content-type

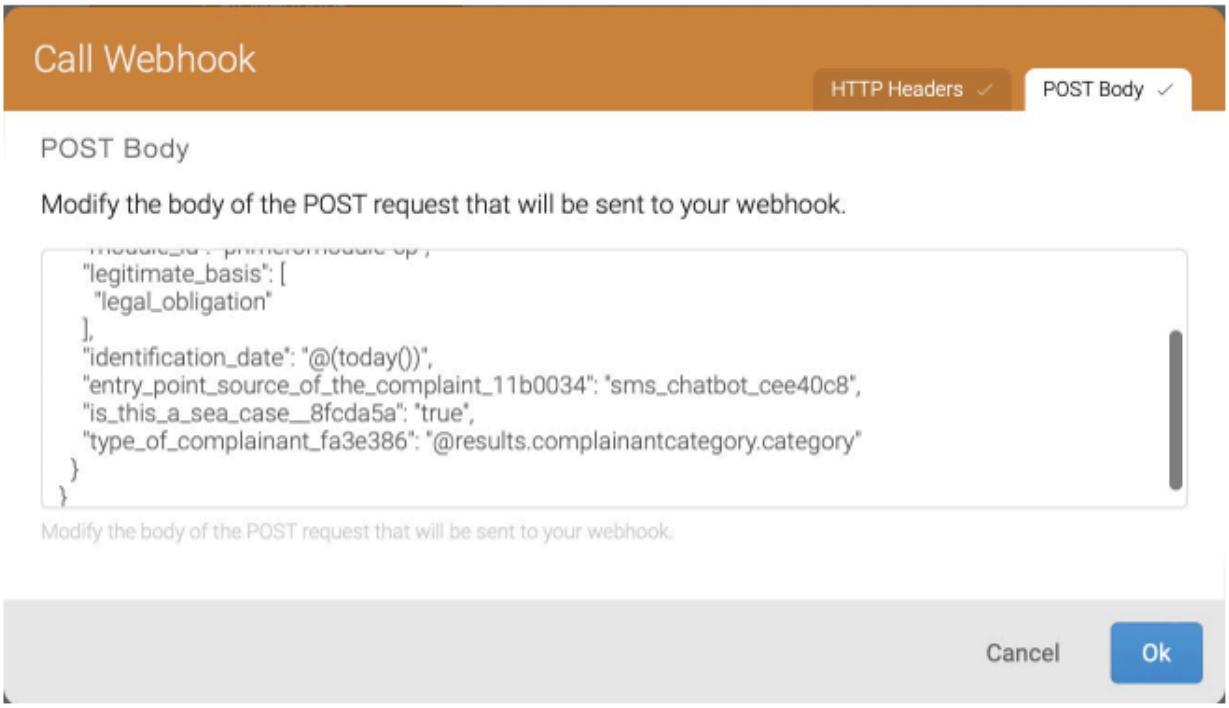
You may find the *accept* and *content-type* headers automatically set. If they are not set, set them to the values in the below screenshot. You will also need to set the *authorization* header. This will reference the global variable you created earlier for the *HTTP Basic Auth* string (in the screenshot, it is called *@globals.primero_auth_string*



In the **post body** tab, we set the data we will send to Primero. It will usually be populated with some pre-existing content when a new webhook node is created, but we will need to set it ourselves.

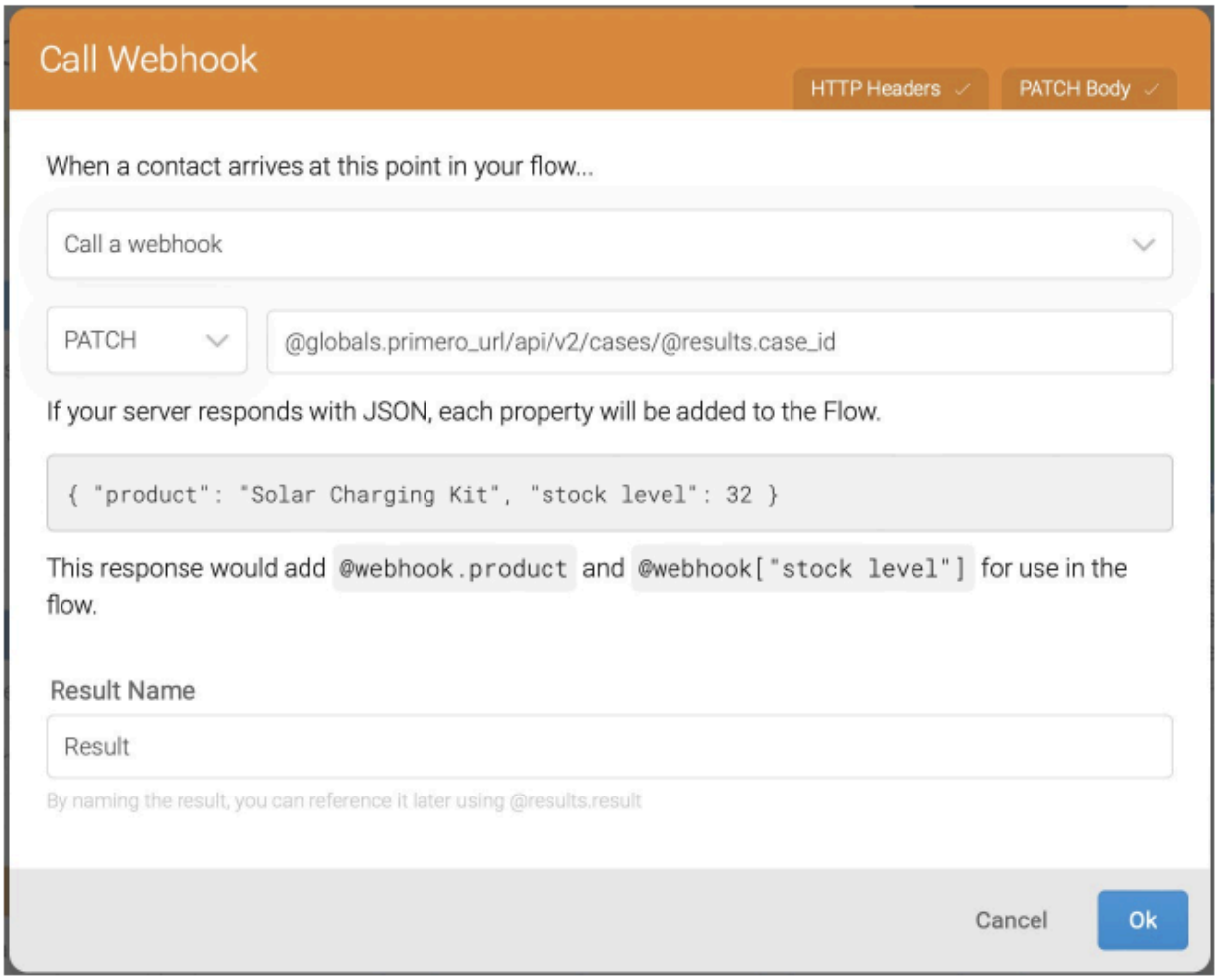
RapidPro uses its own expression language to evaluate templates in flows. The documentation for the expression language can be found here.

Primero expects JSON to be sent to its API endpoints. This JSON is usually easier to template literally rather than using the JSON function in rapidpro (but care will need to be exercised so as to avoid any risk of quoting errors or injection).



If you are updating a case this is largely similar to creating cases, but instead of a POST request, we will send a PATCH request. The payload is a lot simpler as well.

In the first tab, here the main difference to creating a case is that we specify the case ID in the URL. If the case ID is stored from earlier in a result, you can use that in the url.



In the second tab (http headers), this is the same as for creating a new case.

When PATCHING a case, we only need to provide the fields we want to update. For example, if you have stored a result in rapidpro at *results.consent* and you want to save the category of that result (like yes or no) to Primero, you can do the following. *consent.reporting* is the database name on Primero's side that you want to save your result to.

Primero System Settings Configuration for Software Teams and Developers Only

Primero is an information management system that allows for data entry and reporting for child protection, GBV case management and protection case management. The system helps intake relevant information via multiple sources, consolidates the information into relevant record types (Cases / Incidents / Tracing Requests) and allows service providers to report and make educated decisions to assist in these locations.

In version 1 of Primero, there were many features that needed to be updated by a developer. In v2, many of these features are enabled through the front-end UI for system administrators to be able to manage their programme. This includes:

- User management functionality (ability to create and edit users, user groups, agencies and roles which include the ability to manage sending email notifications, creating an incident from, adding a service to a case/incident you do not own, ability to see the view page or “short form” to preview a case, a case or receiving approvals for assessments, case plans or case closures)

- Customizable forms and lookups functionality (ability to create and edit forms and lookups including the ability to reorder form groups, delete subforms or make a field required)
- Locations management (ability to upload locations that will appear in dropdown lists)
- Updating the Code of Conduct, Terms of Use and Support pages

Though many configuration choices can be made directly by a system administrator or a Primero Technical Team member, there are configuration choices that can be requested for a new deployment of Primero which must be made by a developer.

Languages

When deploying a new instance of updating an instance of Primero, system administrators, or focal points responsible for setting up the instance, can request languages to suit the programme/context. Application strings must be translated through Transifex. Forms can be translated through Transifex or through the Forms editor. Languages have corresponding locale codes for example:

- 'en': English
- 'fr': Français
- 'ar': Arabic
- 'ar-LB': Lebanese Arabic
- 'so': Somali
- 'es': Spanish
- 'bd': Bangla
- 'id': Bahasa / Indonesian
- 'ku': Kurdish

This is key to note, as these locales will be referenced and used when importing locations.

Reporting Location Configuration

The "Reporting location config" in the System Settings sets the location levels used for the Dashboard and Filters. Note the "role" permission which has a reporting location for

the role technically overrides it. As a developer, you can include multiple admin levels in 1 label. For example, you can include "'1' => [governerate, camp]" and then both governerates and camps will be included. Note that these options need to be included in the **location type lookup** and typed exactly as they appear in the location type lookup.

```
reporting_location_config: {
  field_key: 'owned_by_location',
  admin_level: 2,
  admin_level_map: { '1' => ['province'], '2' => ['district'] }
},
```

If you would like the dashboard to not display registered cases by district, the dashboard can be updated by a developer to display cases by the current location of the child (db: current_location). To do this, update the field_key to 'current_location'.

Search by ID

Search by ID modal is a pop-up that allows users to search by an ID before creating a case. This can be turned on and off in the Modules:

```
module_options: {
  allow_searchable_ids: true,
},
```

Search Bar

The fields which are used in the search bar are configurable. For instructions on which fields are searchable and how to modify those fields go to the instruction here: https://community.primero.org/t/how-can-i-see-what-fields-are-searchable-how-do-i-refine-my-searches-so-i-only-pull-back-relevant-data/526

Composite Case ID

Composite Case ID can be updated to a specific format requested by the programme which ends in a 7-figure Case ID GUID (case_id_display). For example, the programme may request "Registration Date" and "Case ID" which would look like "12/24/2022/u8347di". For instructions on how to update this in v2, follow steps in this instruction: https://community.primero.org/t/modifying-the-composite-id-in-primero-v2/531

IDs in Primero

The Long ID (case_id) is a 26 character long series of characters generated by an algorithm and virtually guaranteed to be unique. This makes for a convenient means of finding a very specific record. Since this series of characters is so long and hard to remember, though, there is also a Short ID (short_id), which is simply the last seven characters of the Long ID. Both Long ID and Short ID are automatically included in all exports as a means of distinguishing between records. Another identifier that is important is the Case ID (case_id_display) which is a series of characters determined by a pre-set formula which, while still keeping the individual behind the case anonymous, should be more recognizable to a worker. For instance, the Case ID could be the abbreviation for the district where the record was registered plus a dash, the last letter of the child's first name, the day of the month when the child was born, and the Short ID. Such a pattern gives no vital information about the individual, but allows the case worker to distinguish easily between records. The Case ID is displayed on the case list view and is searchable in the search bar. Lastly, Record ID (id) is the key ID of the case which is on the database and is the same series of letters and numbers seen in the in URL. This is another unique identifier for a case.

Age Range

The age ranges can be updated through the system settings by a developer by updating these fields:

```
age_ranges: {
    primero: [0..2, 3..4, 5..9, 10..12, 13..14, 15..17, 18..999],
    unhcr: [0..4, 5..11, 12..17, 18..59, 60..999]
  }
```

Alerts

You can update the label for the alerts for Assessment, Case Plan and Closure for each language in Primero. For example for English you can change the approval labels here:

```
approvals_labels_en: {
    assessment: "BIA",
    case_plan: "Case Plan",
```

```
    closure: "Closure",
    action_plan: "Action Plan",
    gbv_closure: "GBV Closure"
  },
```

You can also set which forms have the alerts appear, for example, you can change alerts to appear on “Basic Identity”:

```
approval_forms_to_alert: {
   assessment_status: 'assessment',
   cp_case_plan: 'case_plan',
   closure_form: 'closure'
 },
```

You can also turn off all alerts:

```
show_alerts: true,
```

Emails

There are notification emails which can be turned on or off for any functionality regardless of the “User” receiving emails:

```
notification_email_enabled: true
```

Welcome email is set at the deployment and can be turned off in the user profile:

```
welcome_email_enabled: true,
```

The content of the Welcome Email can be configured in the “welcome_email_text:” and is pre-configured in the baseline.

Data Protection and Privacy/Legitimate Basis

“data_protection_case_create_field_names” should be an empty array if you would like to turn this feature off.

Full Name Field

By default the PCMIMS+ includes an open text field for users to enter the Full Name. The Full Name field is not editable. The property to add to the field in the config is

hidden_text_field with a value of true or false. And this can also be turned off in the Forms section as an administrator.

Services Tasks

Another attribute in the System Settings portion of the configuration bundle which cannot be edited through the administrator interface is that which controls how services become due. The 'due_date_from_appointment_date' attribute, set to be false by default, can be manually set to true in order to make each service become due based on the the "Appointment Date" field (or any field on the services subform with the id "service_appointment_date"). When this attribute is instead set to false, a service instead comes due based on the "Implementation Timeframe" field (or any other field on the services subform with the id "service_response_timeframe").

API

In order to set up the API role properly you will follow these steps:

1. The development team will set up a API form. This form will be composed of fields that should be shared for interoperability.
2. The development team will set up a role for interoperability. The role itself will need to be provided both read and edit access to the forms needed for interoperability such as the API form, and the the Services form (if you are doing service referrals).
3. The development team will set up a user for interoperability using the above role.

If a time sync is needed OpenFn can set this, and the webhook can be triggered every time an update is made on a case.

All API documentation can be found here: https://github.com/primeroIMS/primero/blob/master/doc/api.md

Workflow Status Bar

A combination of lookups and attributes in the System Settings can be used to control the various workflow statuses that a case can have. Please note that any changes to

the workflow statuses should only be made after significant testing on VMs and discussion with the local steering committee.

Three workflow statuses are always enabled, and will display in the workflow bar no matter what values exist in the lookups. These are "New," "Reopened," and "Closed." It is important to note that only one of the first two of these will display at a given time, with "New" appearing in the bar by default, and "Reopened" only appearing if the case has been reopened after being closed. In this scenario, the "New" status will not appear at all.

Some statuses (associated with the service currently being implemented) come from the "Service Response Type" lookup. The default values for this lookup are "Care plan," "Action plan," and "Service provision." However, any entries made here will appear in the workflow status bar. If a user adds a non-implemented service to an open case and gives it a response type, the case's workflow status will be set to this new service's response type. For example, if I have an open case, and I have added a service that has not yet been implemented and has a response type of "Action plan," the workflow status for the case will then be "Action plan." If multiple non-implemented services have been added, the case's workflow status will be the response type of the most recently-added service. Note: Since the settings in the following section can only be set manually in the user bundle, this section is only for developers working on the user bundle.

There are three more potential workflow values: "Assessment," "Case Plan," and "Service Implemented." Although none of these are set to appear in the workflow status bar by default, each can be enabled for a given module using the use_workflow_assessment, use_workflow_case_plan, and use_workflow_service_implemented attributes, respectively, for whichever module where you want to use the status. Set any one of these attributes to true to use the corresponding workflow status. For instance, to enable the "Assessment" workflow status in the default configuration bundle, search for "PrimeroModule." You should come to a list of all the modules in the system. By default, there should be only one, with an id of "primeromodule-cp." Within the object representing this module, set the use_workflow_assessment attribute to true. You may end up with something looking like the lines pictured below. If you then re-import the bundle with this change, you should see the "Assessment" workflow status show up in the workflow status bar.

For example, case plan and service implemented are turned on if:

use_workflow_service_implemented: true,

use_workflow_case_plan: true,

use_workflow_assessment: false,

Enabling Field Mode

system_settings = SystemSettings.current

system_settings.system_options['field_mode'] = true

system_settings.save!

Adding Other Reportable Fields

Within the reports you are able to generate reports based on the locations listed below:

We also are able to generate a report by:

- Created-by user
- Owned-by user
- Created-by user groups
- Owned-by user groups

In order to enable these fields, here are the ids of the fields found in the standard interagency "Other Reportable Fields" form:

- Created_by
- Owned_by
- Created_by_groups

- Owned_by_groups

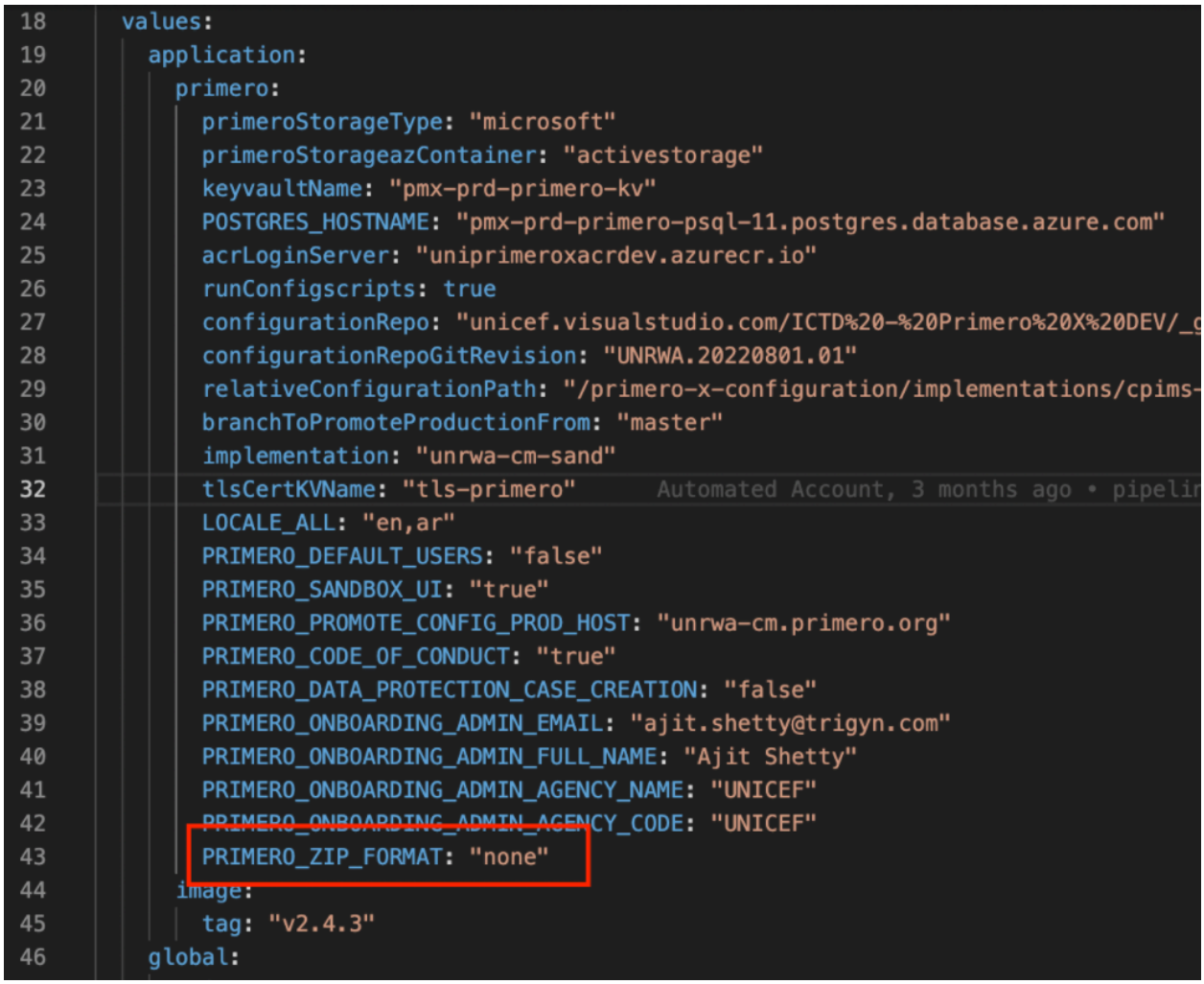
Note that some of these may actually already be found in an implementation's other reportable fields form, and if so, you should just make sure they're formatted the same way as in the interagency forms.

Adding IDP

Documentation: https://unicef.visualstudio.com/ICTD-PRIMEROX-IM/_wiki/wikis/ICTD-PRIMEROX-IM.wiki/2584/Primero-Manual-Changes-for-Developers

Remove Password Encryption from Exports

In the Helm release, developers can disable password encryption by updating the PRIMERO_ZIP_FORMAT;"none"



Turning on alerts and email notifications for updates on a case by a non-record owner

Field in SystemSettings that takes a list of the fields to send the email alerts on. The form has to be added to the list in settings.

A caseworker is assigned to a case where they have some shared responsibility with another agency. There is a different worker that is part of a different agency that gets referred onto the case. That different worker will update certain fields on the case which will trigger an alert (and email) to be sent to the original case worker. If the original case worker then subsequently changes those fields, the other agency case worker will get alerted.

Frequently Asked Questions

How do I set up Primero to test out Referrals?

When testing out Primero's referral functionality, you may decide to set up some test agencies, roles, and users, so that you can fully play out the referral workflow: planning a service, referring the case, logging in as the referral recipient and accepting the referral, then finally recording service details and marking the service as done.

Here are the configuration items you will want to put in place before performing the referral workflow:

- Roles:
  - You will need two roles: one for the user sending the referral, and another for the user receiving it.
  - Sending the referral (typically the case worker role):
    - The role of the user sending the referral should have the **Case > Refer Case from Service** subform permission
    - This role should also have edit access to the **Services** form.
  - Receiving the referral (typically the service provider role):
    - The role of the user receiving the referral should have the **Case > Receive Referral** permission. Also make sure this user has access to adequate forms on the case, including the Services form.
- Agencies:

    - Make sure the agency of the user receiving the referral is listed as providing whatever service you want to refer the case for. For instance, if you want to refer for a **Medical Service**, make sure one of your agencies has this service listed.
- Forms:
    - In the Services subform, make sure the following fields are visible:
        - Type of Service
        - Implementing Agency
        - Service delivery location
        - Service provider name
        - Service implemented (select dropdown)
        - Service completed (date-time field)
        - Notes on the referral from provider (NOTE: This field is filled out automatically with any notes the service provider records when they mark the referral as “Done.”)
- Users
    - You will need two users: one to send the referral, and another to receive it.
    - Sending the referral
        - Make sure this user gets the role you set up for sending the referral (see above).
        - Also note that it is best to practice sending a referral on a case which this user owns, since only the case’s record owner (or their manager) can see all the referrals in the Referrals form.
    - Receiving the referral
        - Make sure this user gets the role you set up for receiving the referral (see above).
        - Make sure this user belongs to the Agency you set up for providing the service. On a related note, when you create this user, leave the **Services** field blank, and make sure that after creation, the user gets all the same services as their agency. This ensures that when you select a

service for referral (e.g. Medical Services), both the example agency and this user will appear as options in the Services subform.

- Give this user a location which is at the standard “reporting location” level for your implementation. Typically, this is the third administrative level or “District” level. Remember the location for this user, since you will be using it later.

Example

- Login to the test site as a CP/PCM HQ Administrator
  - Set the CP/PCM Case Worker role to have edit access to the Services form and the “Refer from Services subform” permission on Cases.
  - Set the CP/PCM Service Provider role to have edit access to the Services form and the “Receive Referral” permission on Cases.
  - Go into the services subform and make sure that all referral-relevant fields (see list above) are visible. They should also all be enabled, except for “Notes on the referral from provider”
  - Create a new “Hospital 1” agency, with the ability to perform the Medical service type.
  - Create a new user with the CP/PCM Service Provider role. Give them the username “hospital-1-sp” Make them part of the new Hospital 1 agency, and leave the Services field blank, so that they inherit the Medical service type from their agency. Set their location as “Iraq:Duhok:Duhok”
- Login to the test site as the CP/PCM Case Worker to test user.
  - Go to any case for which you are the record owner. Edit.
  - Make sure are consent fields are set to “Yes.”
  - Add a service subform.
    - For “Type of Service, select “Medical”
    - For “Implementing Agency,” select “Hospital 1”
    - For “Service delivery location,” set “Iraq:Duhok:Duhok.”
    - For “Service provider name,” set “hospital-1-sp”
  - Finish adding the service subform, then save the case.

    - In the Services subform, click the Refer button on the service you just added.
    - In the Refer modal, leave a note for the service provider, then click Refer.
- Login to the test site as hospital-1-sp
    - In the dashboard, click on the number for “Total Referrals.” Make sure you see the case which the case worker just referred to you. Click this.
    - Go into the Referrals subform and click the actions button (“...”) on the Referral which has been sent to you. Click Accept, then click through the confirmation modal. Note that you are now responsible for this referral’s service.
    - Edit the case. You can now manually add some information to the service. Save.
    - Now, in the Referrals subform, click the actions button (“...”) on the Referral which has been sent to you. Click Done. In the confirmation modal, leave some information in the notes field. Then click Done to confirm you have finished with the referral.
- Log back in to the test site as the case worker
    - Click the “New & Updated” number in the dashboard. Note that you arrive at a case list which includes the case you had referred previously. Click into it.
    - In the Referrals form, note that it is listed as Done, and that a note has been left there about the service, from the service provider.
    - In the Services subform, note that there is an alert at the top of the form, telling you that someone updated the form.
        - Note that the Service Implemented field has been updated to say the service is implemented, and that the Service Completed date field is set to the current date.
        - Note that the “Notes on the referral from provider” field is filled in with the note that the service provider left in the Referral “Done” confirmation modal.
    - Note that the workflow status has been updated to Service Implemented. NOTE: This workflow status does not appear in all implementations.

[a]Note: This list is not complete. We may add more entries here as we get configuration-related questions from administrators which relate to "Important Lookups."

[b]NOTE: Thus far in Primero v2, we are not using this setting for anything, but I'm leaving this section in here in case we decide to leverage it for Interoperability purposes.

[c]Note, this is deprecated, and we will probably be removing it.