Configuring COmanage Enrollment Flows

This page gives a short overview on COmanage enrollment flows and how to configure the most used cases: invitation and self-signup. More detailed (technical) information on enrollment flows can be found at the COmanage application documentation:

- Enable enrolment flows: How to Configure Enrollment Flows
- Configure an invitation flow: How to Configure an Invitation Enrollment Flow
- Configure a Self Signup Flow: How to Configure a Self Signup Enrollment Flow

Basic Idea

An enrollment flow allows a user (in COmanage also known as a **COPerson**) to enroll into a CO or COU they were not a member of yet. Enrollment flows are not meant to administer group membership; group administrators (group owners) can do that directly through the Group interface of COmanage. Group membership does not infer any special rights to members, whereas CO and COU membership allows access to specific services.

During the enrollment flow, the system makes a distinction between the petitioner and the enrollee. The **petitioner** is the person that started the enrollment flow and the **enrollee** is the subject of the flow. For self-signup enrollment flows, petitioners and enrollees are the same. For invitation flows, the petitioner is the person creating the invitation.

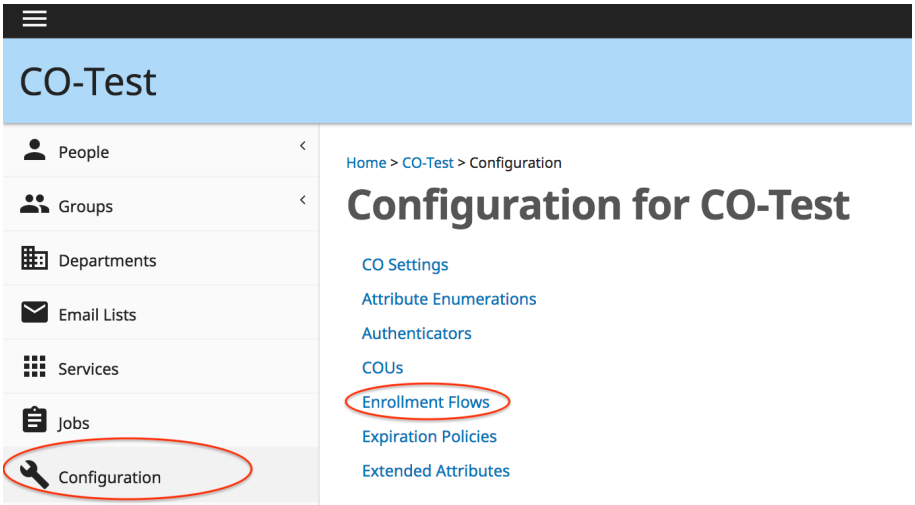
The basic steps of an enrollment flow are:

- creating the petition, entering the relevant values of the enrollee (think of name, email address, organization)
- confirming the email address, which sends an email to the enrollee
- viewing and accepting (confirming) the enrollment by the enrollee
- approving the enrollment by an administrator

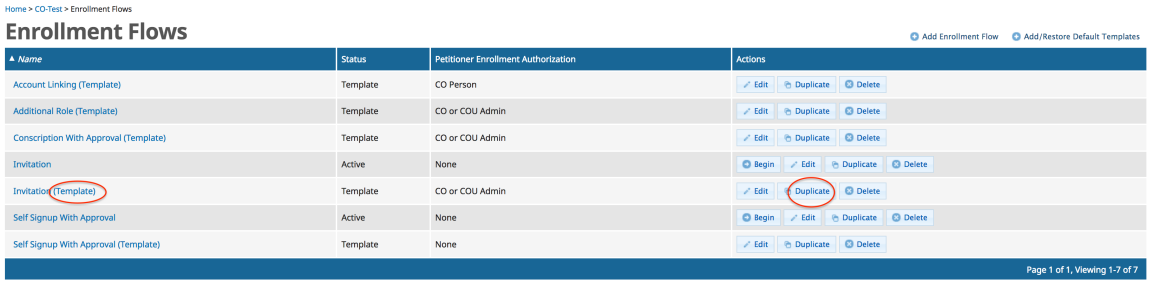
Some of these steps are optional depending on the configuration of the enrollment flow.

Configuration

Enrollment flows reside under the 'Configuration' form of a CO. Only CO administrators can configure these options, other users do not have this link.



New COs do not have any enrollment flows yet, but you can easily add or restore the default templates, which serve as a starting point for further configuration. Before configuring a new enrollment flow, you can duplicate a relevant template.



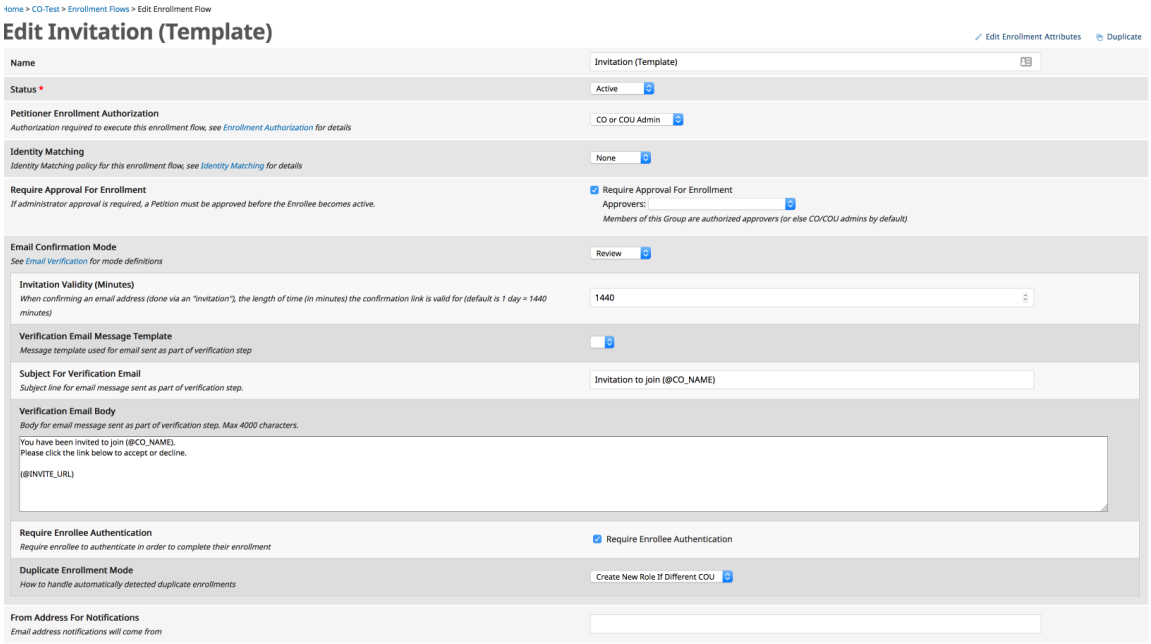
After this, the enrollment flow can be given a name and configured, which requires three steps:

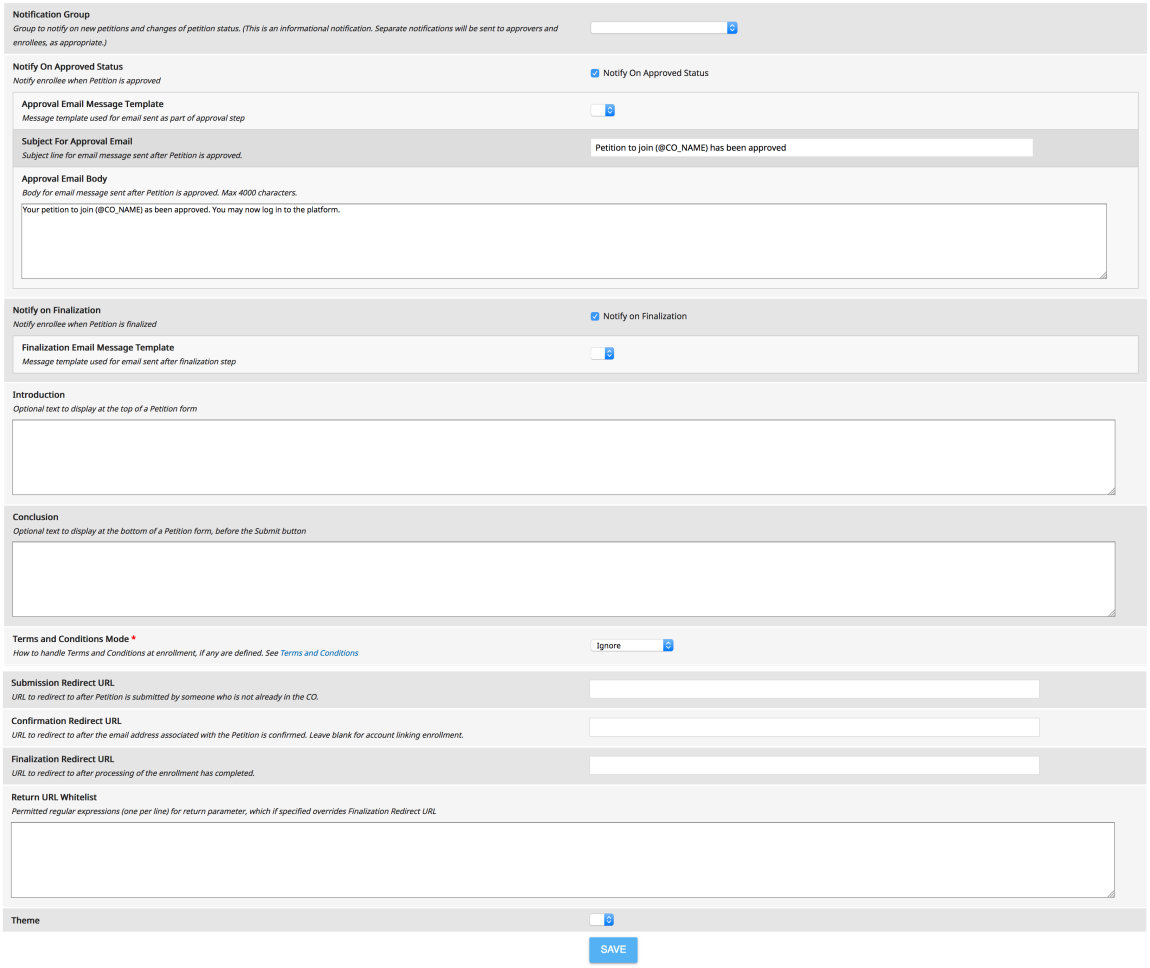
- main configurations
- enrollment attributes
- org-identity-sources

These steps are described in more detail below.

Main Configuration Form

A typical enrollment flow configuration form has the following options selected:





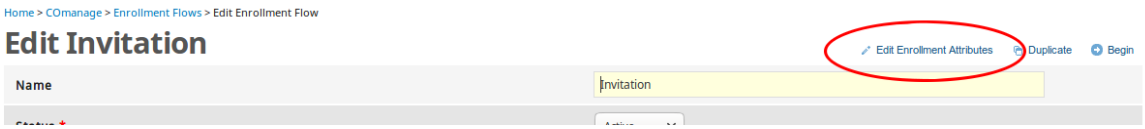
Important fields here are:

- **Petitioner Enrollment Authorization**: this defines who can start the enrollment. For invitation flows, you want this to be set to administrators of the CO or a relevant COU. For self-signup, you normally want this to be 'Authenticated Users'
- **Require Approval for Enrollment**: typically, this is checked to enable administrators to approve individual petitions, although you may want to uncheck this for invitation flows, where approval is done beforehand
- **Email Confirmation Mode**: this determines whether the enrollee can review their enrollment after clicking on the link in the confirmation email. If set to 'Automatic', enrollment proceeds immediately. 'Review' is a sensible setting.
- **Require Enrollee Authentication**: for invitation flows, you want the enrollee to authenticate after accepting the enrollment (review), so the system can gather the IdP provided attributes and this setting needs to be enabled ('on'). For self-signup flows where only authenticated users can enroll, authentication was already done at the start (and the IdP provided attributes were linked), so for self-signup this option can be unchecked ('off').

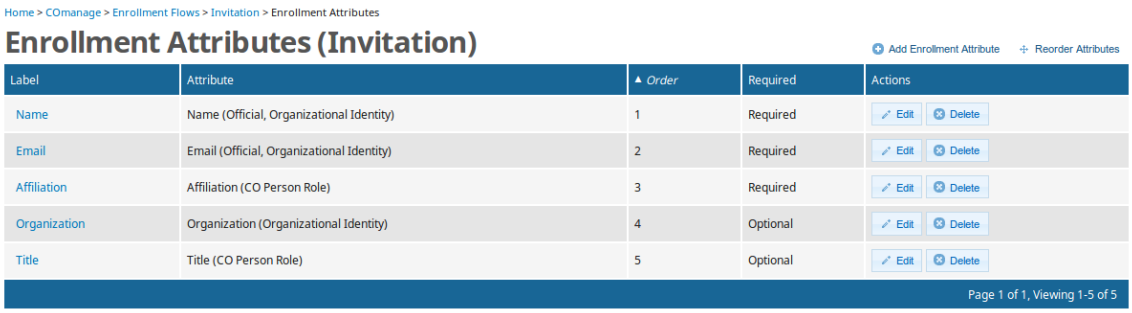
The other fields are either less relevant or very obvious and allow administrators to further personalize the enrollment experience.

Enrollment Attributes

Enrollment attributes determine the attributes gathered of, from or by the enrollee during the enrollment flow:



A typical list of attributes looks as follows:



This list determines which attributes are gathered and to which destination object the attributes are copied (note: **not from which source**). Administrators can determine which values are required, which fields are visible and which attributes can be further modified by the user:

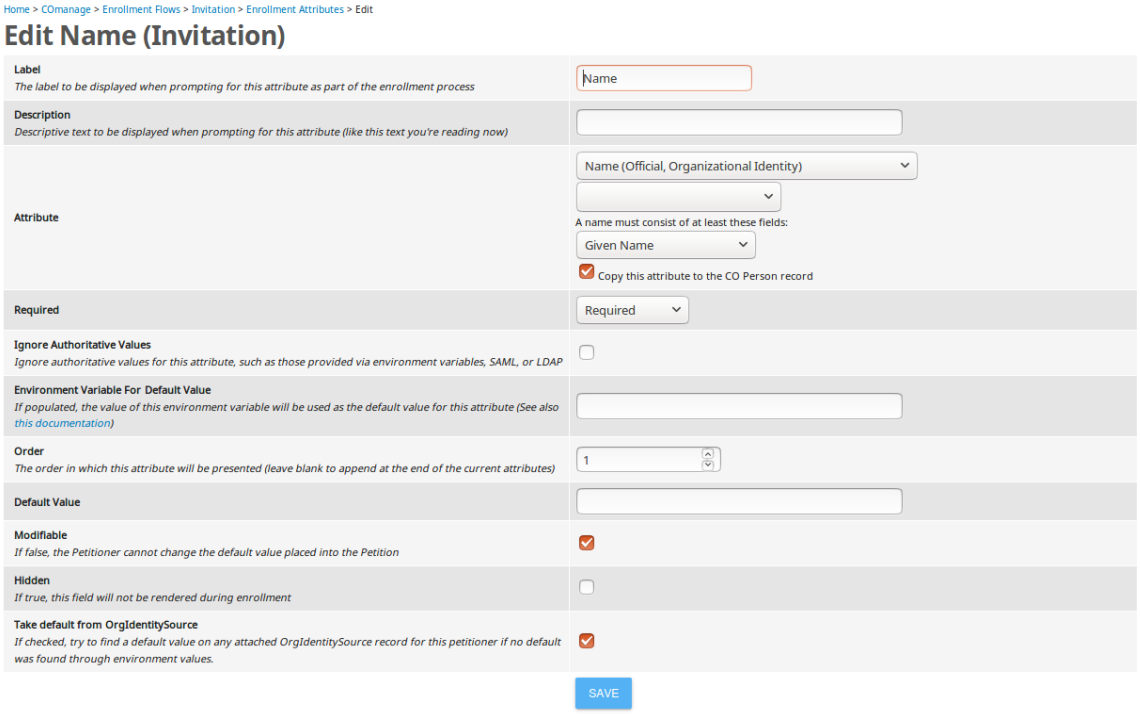
- If using the SamlSource OIS plugin (see below), the authorative IdP attributes are stored non-modifiable in an attached Organisational Identity (OrgIdentity). It is therefore not essential that specific information needs to be non-modifiable to allow administrators to properly identify enrolled COPersons: administrators can always look at the related OrgIdentity with the relevant IdP attributes. This information is clearly visible when perusing an enrolled COPerson's data.
- The SamlSource plugin tries to split a displayName field into givenName and familyName, but it uses a simple algorithm. Consider allowing users to modify their name to avoid cases where this automatic splitting fails, or where users have a different preferred name than their officially registered institute name. This opens the door for people that want to impersonate as someone else, but as mentioned above: administrators have easy access to the IdP provided attributes to correct such cases.
- The email address provided by the IdP might not be the preferred address for this specific CO of that COPerson, so consider allowing users to modify their email address. Alternatively, consider adding a hidden field for the official email address and a modifiable field for the preferred email address
- Please note that copying the IdP provided attributes without allowing users to modify (or even see) the values might violate the user consent and/or the institute privacy guidelines, depending on the scope of the CO and additional policies. In general, it is best practice to only filled required attributes using the IdP provided data as default, but allow users to modify their actual value before proceeding with enrollment.
- For invitation flow enrollment, the IdP attributes are not available yet when these attributes are gathered, so there is no way to copy IdP provided attributes.

Note: the following 3 attributes are REQUIRED for any invitation flow:

- Name
- Email
- Affiliation (CO Person Role)

COmanage will happily accept a flow without those attributes, but will then fail to submit the enrollment form with incomprehensible error messages like "Please check the highlighted field", while not of the fields are highlighted.

A typical attribute configuration form looks like this:



Important fields on this form:

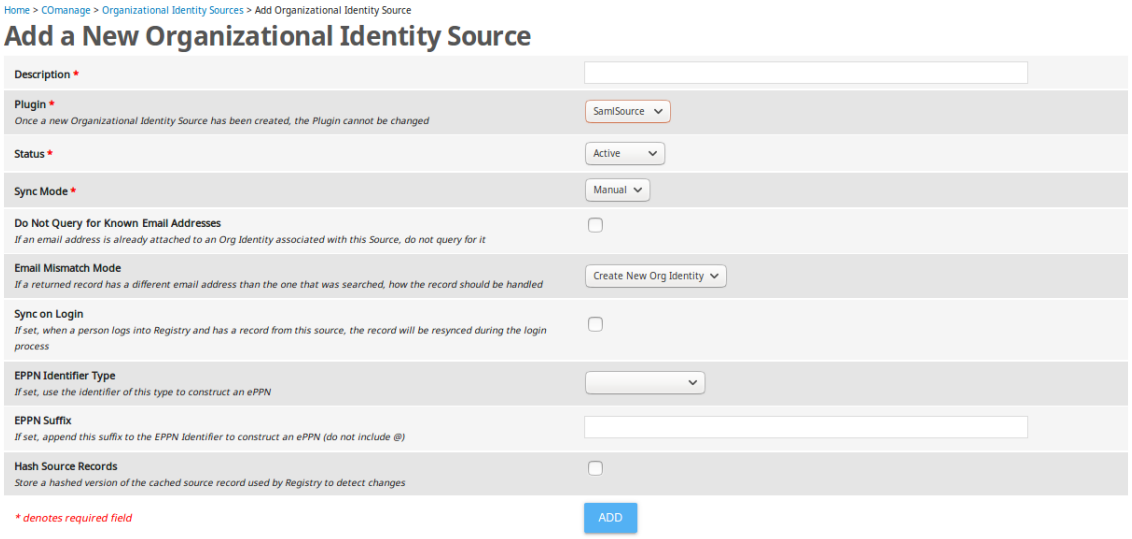
- The attribute you select is the attribute **to** which the gathered data is copied after completing the enrollment-step. For self-signup enrollments, the Organizational Identity attached to the enrollment is a non-modifiable IdP attribute related identity, so you should not select any attributes related to the Organizational Identity (as it cannot be overwritten). Doing so results in non-descriptive user-errors during enrollment.
- Some attributes are related directly to the COPerson (the identity of the user within the bounds of the CO). If a relevant attribute of the Organizational Identity is selected as attribute (in case of invite-flows), this form displays a 'Copy this attribute to the COPerson record' option, allowing you to match Organizational Identity and COPerson identity. This is specifically useful for attributes like name and email address. Note that this option is not available for all attributes, specifically the COPersonRole attributes (that determine the role this person is playing within the bounds of the CO or COU)
- The fields 'Ignore Authoritative Values' and 'Environment Variable for Default Value' can be left off and empty.
- The 'Take default from OrgIdentitySource' option determines if a 'relevant' attribute value is searched for in any attached OrgIdentity for the current enrollment. This matches for example 'preferred email' to 'preferred email', but if no 'preferred email' exists, it will take any email as default. Because of such cases, it is suggested to always allow users to review-and-modify the gathered attributes.
- The minimal required fields for names are either 'givenName' or 'givenName and familyName' and no other options can be configured.
- If you want users to enroll into a COU or sub-COU, you must add an attribute of type COU (COPersonRole)', which allows you to specify the relevant COU. This attribute can be set hidden, non-modifiable, etc. as required. You can add a Group Membership attribute as well, through which you can enroll users directly into the relevant COU admin group to make them administrator. But in general, managing group membership is done elsewhere, in the COmanage group interface. Promoting a COPerson to COU-administrator requires adding them to the relevant COU admin group and can be done outside any enrollment flow.

OrgIdentity Sources

An OrgIdentity Source (OIS) is a data store that can supply relevant OrgIdentity attributes based on some common identifier. COmanage typically uses email address as common identifier, which makes storing the right email address more of an issue.

COmanage has a default OIS called 'EnvSource', which allows reading 'environment variables' of the webserver to scan for relevant authentication attributes introduced by back-end authentication systems like Shibboleth, auth_mod_mellon, etc. Because these variables are hidden from basic CO administrators and can differ based on the original IdP against which is authenticated, use of this specific OIS is not supported by SCZ.

Instead, SCZ supplies the SamlSource OIS. This OIS reads all relevant SAML attributes from the SCZ flow and creates a related, non-modifiable OrgIdentity record. To enable this OIS, you need to configure it under the CO configurations (ConfigurationOrganizational Identity Sources). The form looks as follows:



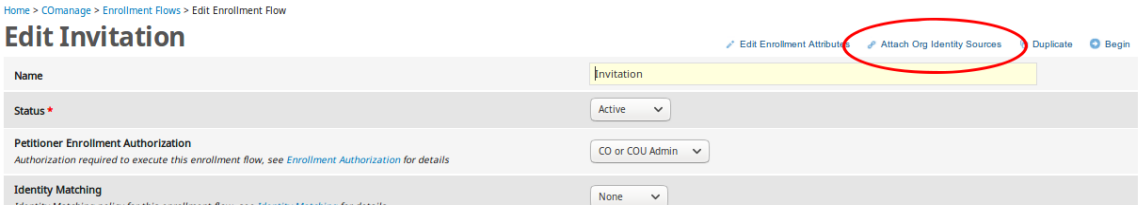
Important fields here:

- select the SamlSource Plugin
- 'Sync Mode' should be 'Manual', because the SAML data is only available when the user logs in and hence cannot be synced when the user is offline
- 'Sync on Login' should be checked ('on')
- SamlSource creates a login identifier based on different settings, so the 'EPPN' fields can be disregarded.
- Detecting changes does not cause any relevant behaviour, so hashing is not required

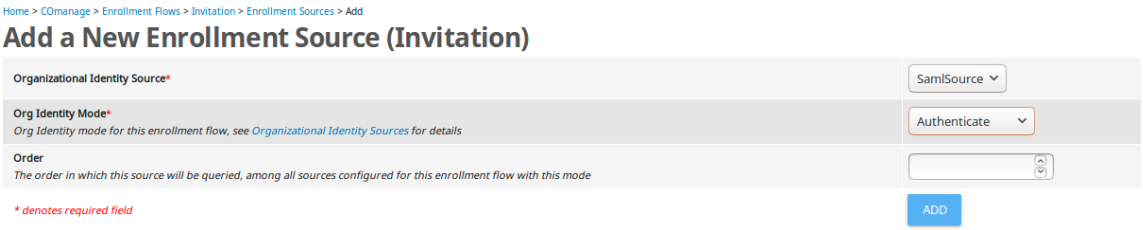
After completing this form, the SamlSource plugin can be setup:

- The Prefix used is 'MELLON_', without the quotes, but including the underscore
- The Identifier used by SCZ is called 'cmuid' (again, without the quotes)

With at least one OIS configured, a new option appears with the enrollment flow configuration screen:



You can add several OIS-es, but the general case is to have only the SamlSource OIS:



Depending on the type of flow, you will need to set the 'Org Identity Mode':

- for invitation flows, you need to set this to 'Identify', so you get an additional OrgIdentity record through which you can identify the enrolled COPerson afterwards
- for self-signup flows, you need to set this to 'Authenticate', so an OrgIdentity is created upon initial authentication, which can be used to set default values for enrollment attributes