Understanding Registry Enrollment and Linking

ⓘ   Before continuing you should first understand Registry people types. You may also wish to review Registry Enrollment (Rev 2, Registry 0.9.4 and later).

Enrollment

Enrollment refers to the process of bringing new person records into the Registry. There are multiple ways to do this, but in the end the result is the same: a new set of attributes about the person is recorded in the Registry. *Invitation* is the default type of enrollment.

Enrollment Flows can be used to customize the enrollment process. Enrollment flows can also add additional Organizational Identities or CO Person Roles to an existing CO Person, through some form of *identity matching*. The execution of an enrollment flow results in the creation of a *Petition*, an artifact that tracks the enrollment and becomes an historical record once enrollment is completed. For day to day purposes, petition attributes are copied to *operational records*, which are editable via the web and REST interfaces.

The following participants are involved in enrollment:

- The **CO Administrator** configures the enrollment flow(s) for the CO.
- The **Petitioner** executes the enrollment flow, creating a petition. The petitioner could be a CO or COU administrator, an existing member of the CO, or a non-member with no existing affiliation to the CO.
- The **Enrollee** is the subject of the petition.
- An **Approver** optionally reviews and approves (or denies) the petition.

Linking

Linking refers to the management of links between existing Organizational Identities and CO Person records. Linking can happen automatically as part of an enrollment process, as described below. However, a CO Administrator can also manually adjust these links, usually to resolve enrollment issues.

Automatic Linking

Registry will attempt to automatically link records during enrollment. This can happen under a variety of circumstances.

Existing Identifier Detected

If an Enrollment Flow is configured with *Authentication Required* and *Require Confirmation of Email*, then the identifier of the currently authenticated user will be collected and attached to the Petition in progress. This identifier will be checked against existing Organizational Identities and an appropriate action taken:

1. If the identifier is not already known, it is attached to the Organizational Identity created as part of the enrollment.
2. If the identifier is known and it is already attached to the Petition's Organizational Identity, no action is taken.
3. If the identifier is known and it is attached to another CO Person within the CO, the action taken is in accordance with the Enrollment Flow Configuration.
4. If the identifier is known, but it is not attached to any CO Person within the CO, the Petition is automatically re-linked to the previously existing Organizational Identity and the new Organizational Identity created as part of the enrollment is automatically deleted.
    a. However, if the new Organizational Identity is already attached to another CO Person within the CO, an error is generated and the situation must be manually resolved.

Self Matching

If an Enrollment Flow is configured with *Identity Matching* set to *Self*, then the enrollment is automatically attached to the currently authenticated CO Person. This is typically used for account linking (adding an additional Organizational Identity) or additional Role enrollment.
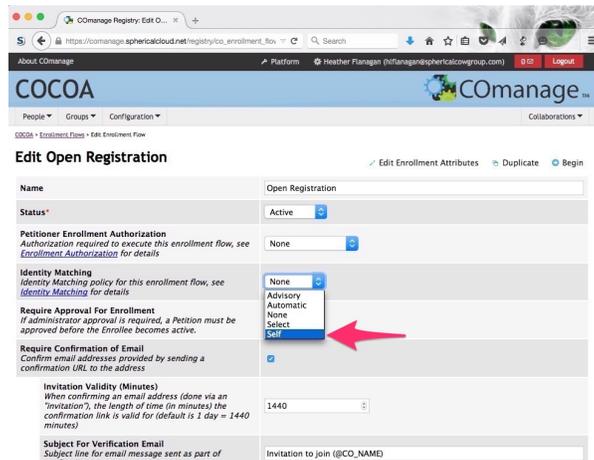
Organizational Identity Sources

[Organizational Identity Sources](#) attached to an Enrollment Flow via [Enrollment Sources](#) can cause [Registry Pipelines](#) to be executed, which can result in automatic linking of records.

Additional Role Enrollment

There are several ways to process an enrollment for an additional role for an already existing CO Person.

1. Via Self Service (presumably with Approval), by setting *Identity Matching* to *Self* and collecting only CO Person Role attributes.
2. Via Administrator Enrollment, by setting *Identity Matching* to *Select* and collecting only CO Person Role attributes.
3. Via existing identifier detection, as described above. Unlike the first two options (which only work for existing CO People), this option can be applied to all enrollees (whether or not they are new to the platform – if they are new, CO Person and Org Identity records will be created as needed).