Registry Enrollment Authentication and Authorization

> ⓘ Before continuing, be sure you have reviewed Understanding Registry Enrollment and Linking and Registry Enrollment (Rev 2, Registry 0.9.4 and later).

Because Registry Enrollment may involve subjects without existing Registry records, authentication and authorization for Registry Enrollment Flows operates a bit differently than for the rest of Registry or other parts of the COmanage Platform. Registry Enrollment can involve multiple steps by various actors, which can be interrupted and re-engaged at various times.

Petitioner

When an Enrollment Flow is started (**Start** step executes), a petition is created and the Petitioner is recorded.

- If *Enrollment Authorization* is configured (ie: not *None*), then the Petitioner is an existing CO Person. The Petitioner's CO Person ID is recorded is part of the Petition artifact.
- If *Enrollment Authorization* is not configured (ie: set to *None*), then the Enrollment Flow is open, and the Petitioner may not be an existing CO Person. A random token is generated to link the Petitioner steps.

For each subsequent Petitioner step of an Enrollment Flow, the following logic is used to determine if the step may be executed:

1. A Platform Administrator, CO Administrator, or COU Administrator (when the Petitioner is in the population of the COU Administrator) may execute the step. This is not always advisable, as depending on the configuration incorrect attributes (those of the Administrator rather than those of the Petitioner) may be collected.
2. If a Petitioner CO Person ID was recorded and the currently authenticated user has the same CO Person ID, the current user may execute the step.
3. If the Petitioner presents a valid token, they may resume the associated Petition.

Enrollee

Currently, an Enrollee only interacts with an Enrollment Flow if *Require Confirmation of Email* is enabled. (This is subject to change in a future release.) As such, the initial interaction requires the Enrollee to present an Invitation ID that was sent via email. Then,

- If *Require Authentication* is true, the Enrollee must authenticate. The identifier obtained as part of authentication is attached to the Petition.
- If *Require Authentication* is not true, then the Enrollee is not required to present credentials. A random token will be generated to link the Enrollee steps.

For each subsequent Enrollee step of an Enrollment Flow, the following logic is used to determine if the step may be executed:

1. A Platform Administrator, CO Administrator, or COU Administrator (when the Enrollee is in the population of the COU Administrator) may execute the step. This is not always advisable, as depending on the configuration incorrect attributes (those of the Administrator rather than those of the Enrollee) may be collected.
2. If an Enrollee CO Person ID was recorded and the currently authenticated user has the same CO Person ID, the current user may execute the step.
3. If the Enrollee presents a valid token, they may resume the associated Petition.

Approver

If an Enrollment Flow requires approval, the set of Approvers is determined by the approvers group of the Enrollment Flow. Any Approver step may be executed by any authorized Approver. (This is subject to change in a future release.)