Registry Enrollment Flow Configuration

About Enrollment Flows and Petitions

Every organization has one or more ways of bringing new people into that organization. There are a number of terms used to described this process: *application*, *enrollment*, *intake*, *invitation*, *petition*, *signup*, etc. These processes vary significantly across organizations.

COmanage Registry has a sophisticated, configurable mechanism for representing these processes, and translating them into ways to bring people into a CO's registry. (You can see a representation of the model here.) COmanage Registry refers to these processes as *Enrollment Flows*, and the execution of these processes as *Petitions*.

Each CO can define as many Enrollment Flows as it needs to reflect it's specific processes, subject to the COmanage platform configuration. (A CO can also use the very basic default mechanism.) When a new person is to be enrolled, the new person (if self-signup is enabled) or an appropriate administrator creates a Petition to begin the process.

See also: Understanding Registry Enrollment and Linking

Default Enrollment (Invitation)

By default, COmanage Registry operates using an invitation-based enrollment flow. As a CO Admin, you can tell this is in effect by viewing "My Population" for your CO. There will be a button labeled "➕ Invite" at the top of the page.

Defining Enrollment Flows

To customize enrollment, select "CO Enrollment Flows" from your CO's menu. You can define more than one flow, to allow for different enrollment processes.

After you define the basic settings of enrollment (see also the table below for common patterns), define the attributes that will be collected as part of this flow.

Once an Enrollment Flow is defined, the button at the top of the "My Population" page will become "➕ Enroll" instead. Clicking that button will present a menu of available Enrollment Flows to execute.

Creating Organizational Identities As Part of An Enrollment Flow

⚠️

⚠ Beginning with Registry v5.0.0, it will no longer be possible to manually create Org Identity attributes via an Enrollment Flow. Org Identities can be created from Organizational Identity Sources (and Enrollment Sources). Prior to this change, it is recommended that new Enrollment Flows not use Org Identity attributes.

See also: Consuming External Attributes via Web Server Environment Variables.

For COs that will not collect Organizational Identities from authoritative sources (ie: via LDAP or SAML), Enrollment Flows must be configured to collect this data. In order to allow this, the platform must be configured to enable this, via these instructions. ⚠ Most deployments will likely need to enable this setting. As of v0.9.3, this setting is enabled by default.

Once enabled, CO administrators will be able to add Enrollment Attributes to a CO Enrollment Flow with the type "Organizational Identity".

To facilitate data entry, certain Enrollment Attributes can be configured once in an Enrollment Flow, but populate both the Organizational Identity and the CO Person record. When such an attribute is selected, the option "Copy this attribute to the CO Person record" will become available (as part of editing the Enrollment Attribute).

(See also the platform configuration Pooling Organizational Identities.)

Enrollment Flow Attributes

An Enrollment Flow is just a process for assembling attributes about a person and storing them in records used for day to day operations. Generally speaking, any attribute that can be managed operationally by COmanage Registry (whether attached to a CO Person, a CO Person Role, or an Organizational Identity) can be collected as part of an Enrollment Flow.

The following attributes must be defined for a "complete" enrollment:

- COU, if COUs are enabled, and if a new CO Person Role is being created (eg: not needed for account linking)
- Org Identity Name (see note below)
- Org Identity Email Address
- CO Person Name (see note below)
- CO Person Role Affiliation, if a new CO Person Role is being created (eg: not needed for account linking)
- See also the note below (Email Verification and Authentication) about automatically populating ePPN (no need to explicitly define an attribute for this)
- See also Configuring Registry Identifier Assignment (no need to explicitly define an attribute for this)
- See also Registry Platform Configuration

⚠ You *can* make these attributes optional or unspecified, but for a complete enrollment you probably shouldn't. Making name optional, for example, will allow someone to submit a petition without specifying their name.

For other types of enrollments, however, it may be appropriate to omit certain attributes. For example, an Additional Role Enrollment should only define CO Person Role attributes.

⚠ Exactly one Org Identity Name of type `Official` and exactly one CO Person Name of type `Official` must be specified. (The CO Person Name may be copied from the Org Identity value.)

Additional Names may also be defined (eg: CO Person Name of type `Author`), however no additional names of type `Official` may be defined.

⚠ Enrollment Flows with an Enrollment Source in Authenticate mode cannot currently be configured to collect additional Organizational Identity attributes. (CO-1635)

Default Values For Attributes

Certain attributes configured as part of an Enrollment Flow can be assigned default values. (When editing an enrollment attribute, the form will automatically show default value fields when appropriate.) When a Petition is created from the Enrollment Flow, the default values are pre-populated into the form. Default values can also be flagged as not modifiable, in which case the value loaded into the Petition cannot be changed by the Petitioner.

Currently, the following types of attributes may have default values assigned:

- Single valued Organizational Identity attributes (basically, those defined in cm_org_identities)
- Single valued CO Person Role attributes (basically, those defined in cm_co_person_roles)
  - Special conditions apply to Sponsors and Managers
- Extended Attributes
- CO Group Memberships
  - An Enrollee can only be added to a CO Group as a member ("CO Group Member"), and/or an owner ("CO Group Member and Owner")
    - For "CO Group Member and Owner", the Enrollee will be added as both a member and an owner, except for opt-in groups as described below
  - By setting the default value to be not modifiable, the associated CO Group is fixed; otherwise a Petitioner can add the Enrollee to any available CO Group
  - By setting a default value, flagging it as not modifiable, not hidden, and optional, the CO Group becomes opt-in (by the petitioner)

- For "CO Group Member and Owner", either or both roles may be selected for opt-in

If the selected attribute has Attribute Enumerations defined for it, the default value can only be chosen from one of the enumerated options.

Attributes that represent dates can receive default values based on

- A fixed date (eg: June 30, 2013)
- The next occurrence of a date (eg: next June 30)
- A specific number of days from the creation of the petition (eg: in 90 days)

In addition, if the Enrollment Flow is configured for *Self* matching (described below), the Petitioner's name will be pre-populated into the Organizational Identity name fields.

Populating Attributes From Authoritative Sources

Certain attributes can be collected from authoritative sources, such as a SAML assertion.

Self Selected Identifiers

Limited support for self-selection of identifiers during enrollment is available via the IdentifierEnroller Plugin.

Timezones For Validity Timestamps

When configuring Valid From and Valid Through attributes, keep in mind that the timestamp entered by the Petitioner will be considered to be in the local timezone of the Petitioner, and then converted to UTC to be stored in the database. See Understanding Registry Timezones for more information.

Enrollment Flow Templates

An Enrollment Flow Template is simply an Enrollment Flow that is not Active (and therefore cannot be executed), but can be duplicated to create additional Flows. Any existing Flow may be turned into a Template. (Active Flows may also be duplicated.)

COmanage Registry includes several default Templates. To instantiate these, go to *Configuration >> Enrollment Flows* and click *Add/Restore Default Templates*. Note that while the default templates are functional, they are unlikely to be useful for most needs. They are best thought of as starting points, with customization recommended in accordance with the needs of a given deployment.

Petitions and Petition Attributes

The process of executing an Enrollment Flow creates a Petition. The Petition is the record of enrollment – it holds copies of the attributes that were provided at enrollment, even if the values are subsequently changed. History records are also maintained for the Petition, indicating such events as who approved it and when.

Petition-Specific Attributes

It is possible to collect additional attributes as part of an Enrollment Flow that stay within the Petition, but do not become part of the CO Person's operational record. For example, an Enrollment Flow might ask an applicant to provide a sentence explaining why they are interested in joining.

These Enrollment Attribute types are labeled "(Petition Use Only)" when adding a new Enrollment Attribute to an Enrollment Flow.

Enrollment Authorization

Various authorization levels can be selected to determine who may initiate a given Enrollment Flow.

- **Authenticated User**: Any authenticated user, whether or not there is an existing CO Person record.
- **CO Admin**: Only a CO Admin for the CO. CO Admins can always initiate any Enrollment Flow within the CO.
- **CO Group Member**: Any member of the specified CO Group.
- **CO or COU Admin**: Any CO or COU Admin in the CO.
- **CO Person**: Any person who is a member of the CO.
- **COU Admin**: Any COU Admin for the specified COU.
- **COU Person**: Any person who is a member of the specified COU.
- **None**: No authorization required. Useful for self-signup patterns.

Any setting other than *None* will trigger authentication if the user is not already authenticated. ⚠ If you are collecting Web Server Environment Variables, you will need to select an authorization level other than *None.*

Enrollment Flow Visibility

Prior to Registry v3.2.0, all logged in users can obtain a list of available Enrollment Flows via *People >> Enroll.*

As of Registry v3.2.0, this menu is no longer available to non-Administrative users. Links to specific Enrollment Flows can be made available in the *My Identity* menu by ticking the *Enable My Identity Shortcut* setting.

Identity Matching

COmanage Registry can perform identity matching when enrollment is performed. This is the process of checking for existing CO People that might match the person being enrolled. Note that matching only happens during the execution of an enrollment flow, now when manually adding a new CO Person. The following matching policies are available:

- **None**: No matching is performed.
- **Advisory**: Potential matches are identified, but Registry does not take any action. See more on Advisory Matching, below. This should only be enabled for Administrator (or other trusted user) driven enrollments.
- **External**: Matching is processed using an external match service. See Integrating With ID Match.
- **Select**: The Petitioner chooses an existing CO Person from the list of all CO People. This is useful for additional role enrollment, and should only be enabled for Administrator (or other trusted user) driven enrollments.
- **Self**: The new enrollment is automatically linked to the Petitioner. Used for self service account linking and additional role enrollment.

> ⚠ For Self matching, at least one of **Require Authentication**, **Require Confirmation of Email**, or **Require Approval** must be enabled in order for the enrollment to proceed from Pending Approval status to Active.

> ⚠ Enrollment Flow Identity Matching is unrelated to Pipeline Match Strategies.

System of Record Label

See Integrating With ID Match for details on specifying a System of Record (SOR) Label. A SOR Label is not required unless integrating with ID Match.

Advisory Matching

Advisory matching currently only works when the following conditions are met:

1. *Advisory* matching is configured for the enrollment flow.
2. The field where data is entered is either a given or family name field. ⚠ If an enrollment flow is configured to collect more than one type of name, only the *first* set of name fields emitted will be enabled for Advisory Matching.
3. At least 3 characters are entered into the field.

Organizational Identity Sources

Enrollment Flows can be configured to query Organizational Identity Sources for Organizational Identity data, by selecting *Attach Org Identity Sources* in the Enrollment Flow configuration. Such enrollments will result in new Org Identities created, linked to the specified Organizational Identity Source. For more details, see Enrollment Sources.

Duplicate Enrollments

COmanage Registry can detect duplicate enrollments under limited circumstances. (Alternately, duplicates can be manually resolved.) When enrollee authentication is required (see below), the authenticated identifier is used to check for prior enrollments. What happens when a duplicate enrollment is detected is configurable on a per-Enrollment Flow basis:

- **Flag as Duplicate**: The Petition and associated CO Person/Role are flagged as Duplicates.
- **Create New Role**: The CO Person Role data from the Petition is used to create a new Role for the existing CO Person.
- **Create New Role If Different COU**: If COUs are enabled and the CO Person Role data from the Petition is for a COU that the existing CO Person is not already associated with, then a new Role is created for the existing CO Person. Otherwise, the Petition and associated CO Person /Role are flagged as Duplicates.
- **Merge**: The models (Address, EmailAddress, Identifier, Name, TelephoneNumber) associated with the Petition's Org Identity are merged into the already existing Org Identity. CO Person attributes are not currently merged.
  - ⚠ Merge is not supported for Enrollment Flow integration with an external ID Match server.
- **Merge and Replace**: Not yet implemented (CO-1296).

See also Automatic Linking.

⚠ When using EnvSource, use EnvSource's Duplicate Handling mode instead.

Invitations

Invitations are the mechanism by which enrollment is transitioned from a Petitioner to an Enrollee, when the two are not the same person. For example: when an administrator starts the enrollment process for a new participant. Invitations are sent via email, and contain a URL which the Enrollee uses to take over the Enrollment Flow. This means the email address used to deliver the invitation can also be considered verified once the invitation is accepted, but otherwise see *Email Verification*, below, for more information.

As of Registry v3.3.0, the following modes are supported:

- **Automatic**: The Enrollment Flow resumes processing as soon as the enrollee clicks on the email link
- **None**: No invitation is sent
- **Review**: After the Enrollee clicks on the email link, the petition record is displayed for the Enrollee to review before confirming or declining

Email Verification (Confirmation) and Authentication

Email Verification (Confirmation) will result in an email being sent to the email address enrolled. A URL is included in the email, and the enrollee must click on the URL to verify the email address. Prior to v3.2.0, an Org Identity email address must be collected as part of the Enrollment Flow, however as of Registry v3.2.0 the following algorithm is used:

1. If the Enrollee Organizational Identity is *not* associated with an Organizational Identity Source, then look for the first unverified Email Address attached to the Enrollee Organizational Identity to verify. In other words, if EnvSource or a similar mechanism is in use, the Org Identity Email Address will not be selected for verification.
2. Otherwise, look for the first unverified Email Address attached to the Enrollee CO Person to verify.
3. If no suitable Email Address is found, this step will fail.

As of Registry v2.0.0, the following modes are supported:

- **Automatic**: Verification takes places as soon as the enrollee clicks on the email link
  - ⚠️ Note that some email clients may fetch links in a message to preview or cache them. These clients may cause email confirmations to be prematurely used.
- **None**: No verification takes place
- **Review**: After the enrollee clicks on the email link, the petition record is displayed for the enrollee to review before confirming or declining
- **Skip If Verified**: If the Org Identity Email Address is already verified then the CO Person Email Address will be automatically verified and then Enrollee will not be prompted to confirm (available as of Registry v4.0.0)

Authentication requires the enrollee to authenticate as part of the enrollment process. The authentication is linked to the identity via an email invitation, and so authentication currently requires email verification. This may change in a future release.

If authentication is enabled, the authenticated identifier will automatically be added to the Enrollee's Organizational Identity (currently forced to type `ePPN`, CO-460) and flagged for login, if the identifier is not already part of the record. ⚠️ This feature is deprecated, and will be removed in Registry v5.0.0.

⚠️ The Authentication setting is deprecated. The use of EnvSource or a similar mechanism is instead recommended to collect the enrollee's authenticated identifier.

As of Registry v4.1.0, self service resending of confirmation emails may be enabled via the Recovery Dashboard Widget.

Handling Expired Confirmation Links

As of Registry v4.1.0, Enrollment Flows may be configured to *Allow Regeneration of Expired Links*. When enabled, if the enrollee clicks the link in the confirmation message after it has expired (as per *Invitation Validity*), a new confirmation link will automatically be sent to the same email address. (It is not possible to redirect the message to another address.) An appropriate note will be added to the Petition History.

Notifications and Message Templates

Enrollment Flows can trigger various Notifications at key stages, including confirmation, approval (enrollee), approver, and finalization. While these messages could originally be defined in each flow, the preferred approach is to instead defined Message Template, and then reference that template from the Enrollment Flow configuration. The ability to define messages directly in the flow configuration will be removed in Registry v5.0.0 (CO-1213).

Terms and Conditions

COmanage Registry can require agreement to Terms and Conditions as part of an Enrollment Flow. Authentication must be required.

Redirect Targets

At certain points in an Enrollment Flow, it is possible to define Target URLs where the petitioner or enrollee is sent.

- After a Petition is submitted, if the Petitioner is not already a member of the CO (eg: self signup), then the Petitioner will be sent to the URL specified via **Submission Redirect URL** (if any).
- After the Enrollee confirms their email address (by clicking the link sent to them), they will be sent to the URL specified via **Confirmation Redirect URL** (if any).
  - This setting should **not** be used for Account Linking enrollment.
- After the enrollment process has completed, the actor will be sent to the URL specified via **Finalization Redirect URL** (if any).
  - If email confirmation is required *and* approval is not required, this setting will have no effect. Use *Confirmation Redirect URL* instead.
  - If approval is required, the Approver will be redirected to the specified URL, not the Enrollee.
  - This setting is available from Registry v3.1.0.

When a redirect is issued to one of these URLs, the session variable `CoPetition.id` will also be set. This allows a potential target URL within COmanage Registry to determine which Petition is currently in process. This is particularly useful for custom Plugins that wish to add functionality to the Enrollment Flow. ⚠️ This functionality is no longer present from v0.9.4. Use Enroller Plugins instead.

Target URLs outside of the Registry environment will not have access to the petition information.

> ⓘ For relatively static content with the Registry look and feel, considering using the public content capability.

Petition-Specific Redirect Targets

As of v3.1.0, it is possible to specify a redirect target when a Petition is first created. If set, this target will be used instead of the Finalization Redirect URL (as described above). ⓘ As of v3.3.0, Petition-Specific Redirect Targets are also supported in place of the Confirmation Redirect URL.

Permitted redirect URLs must be permitted using the Enrollment Flow's *Return URL Allow List* configuration, which is a list of regular expressions, one per line. Example allow list values:

```
/^https?:\/\/.*\.myvo\.org/
/^https:\/\/myvo\.org\/idp/
```

Then, append a `return` parameter to the Petition start URL, Base64 encoding the desired return URL. For example:

```
https://registry.mvyo.org/registry/co_petitions/start/coef:203/return:aHR0cHM6Ly9teXZzvLm9yZy9pZHANCg--
```

If the decoded return parameter does not match an allow list entry, it will be ignored.

> ⚠ There are two important considerations to remember when using Petition Specific Redirect Targets:
>
> 1. Filtering is not performed on the URL when it is issued. As such, the allow list should be tightly constrained to limit what URLs can be supplied for the `return` parameter, including what parameters or valid characters can be provided. (Keep is mind allow list validation does not occur until the redirect is issued, so it is possible to submit invalid URLs, but they will be ignored.)
> 2. Base64 encoding can result in URL special characters, specifically +, /, and =. There is no universal way to handle this, so Registry (as of v3.2.0) maps these to ., _, and − respectively. ("plus" becomes "dot", "slash" becomes "underscore", and "equals" becomes "dash".) In PHP, you might do something like this:
>
> ```
> $returnParam = str_replace(array("+", "/", "="), array(".", "_", "-"), base64_encode($myUrl));
> ```

Establishing Authenticators

As of Registry v3.3.0, Authenticators (such as Passwords and SSH Keys) may be established by the Enrollee. In order to do so:

1. Configure the desired Authenticators, if not already done.
2. In order for the Enrollee to be able to establish their Authenticators, the Enrollment Flow must be configured with Email Confirmation enabled.
3. Enable *Establish Authenticators* in the Enrollment Flow configuration.
4. Set the desired mode for each Authenticator:
   - Required: The Enrollee must successfully establish the Authenticator in order to continue the flow.
   - Optional: The Enrollee may establish the Authenticator, or may click *Skip* to move on to the next step.
   - Not Permitted: The Authenticator will not be established during the flow.

⚠ The Enrollment Flow must already have been saved before Authenticators can be attached. ie: It is not possible to configure *Establish Authenticators* while adding a new Enrollment Flow, only when editing an existing one.

Establishing Cluster Accounts

As of Registry v3.3.0, Cluster Accounts may be established by the Enrollee. In order to do so:

1. Configure the desired Clusters, if not already done.
2. Edit the configuration for the desired Enrollment Flow, and tick *Establish Cluster Accounts*.
3. Tick the checkbox for each Cluster on which an Account should be created during enrollment, and save the configuration.

⚠ The Enrollment Flow must already have been saved before Clusters can be attached. ie: It is not possible to configure *Establish Clusters* while adding a new Enrollment Flow, only when editing an existing one.

Vetting

As of Registry v4.1.0, Person Vetting may be run as part of Enrollment.

Comments

Administrators reviewing a Petition may add comments to the petition. To do so, retrieve the appropriate Petition and click "Add Comment". The comment will be visible in the Petition History (to anyone with permission to view Petition History).

Approval

An Enrollment Flow can require approval before an Enrollee becomes active. If approval is enabled, then the following people may approve a Petition:

1. Any CO Person that is a member of
   a. an explicitly configured group set under *Require Approval For Enrollment* or
   b. the Approvers Groups, if defined
2. Otherwise

a. Any CO Admin for the CO may approve the Petition
b. A COU Admin may approve the Petition when one of the following conditions is met
   i. If the Enrollment Flow defines a specific COU whose COU Admins may execute the flow, then any of those COU Admins may approve the Petition
   ii. If no such COU is specified but the Petition is attached to a COU (via an Enrollment Flow Attribute), then COU Admins for that COU and all parent COUs may approve the Petition
   iii. If no specific COU is defined, then any COU Admin for the CO may approve the Petition.

CO Person Status

When a Petition is approved/completed and the associated CO Person Role becomes active, the overall status for the associated CO Person will be recalculated.

Enrollment Flow Plugins

Enrollment Flows can be further customized by the use of Enrollment Flow Plugins. As of Registry v4.0.0, Enrollment Flow Plugins must be *instantiated*, meaning they must be attached to a specific Enrollment Flow to be used. An Enrollment Flow Plugin attached to an Enrollment Flow is called an *Enrollment Flow Wedge*. Enrollment Flow Wedges are managed using the *Attach Enrollment Flow Wedges* link on the Enrollment Flow configuration page.

Enrollment Flow Wedges may be ordered. If more than one Wedge will run at a given Enrollment Flow execution point, the ordering will be used to determine which plugin is run first.

Updating Enrollment Flow Configurations

In order to maintain historical accuracy and consistency, when a Petition is created it is permanently linked to the Enrollment Flow configuration at the time the Petition is created. If the Enrollment Flow configuration is subsequently updated before the Petition is completed, the new configuration will *not* be applied to the existing Petition. In progress Petitions can manually be denied or terminated to prevent this behavior, though it may also be necessary to expunge partially created person records.

See also: Changelog Behavior

Common Enrollment Patterns

Pattern	Conscription	Invitation	Self-Signup	Application	Account Linking
Description	Petitioner adds enrollee, possibly with CO admin approval but without enrollee confirmation.	Petitioner adds enrollee, possibly with CO admin approval. Enrollee confirms before becoming active.	Enrollee is also petitioner. No approval processes needed for enrollee to become active.	Enrollee is also petitioner. Approval processes required before enrollee is active.	Enrollee is also petitioner. Enrollee already exists in the CO, and wishes to add an additional organizational identity.
Enrollment Authorization	Any other than **None**	Any other than **None**	**None**	**None**	**CO Person** or **COU Person**
Identity Matching	Any other than **Self**	Any other than **Self**	**Automatic** or **None**	**Automatic** or **None**	**Self**
Require Approval for Enrollment	*Optional*	*Optional*	*Optional*	**Yes**	**No**
Require Confirmation of Email	*Optional*	**Yes**	*Recommended*	*Recommended*	**Yes**
Require Authentication	*Optional*	*Optional*	*Optional*	*Optional*	**Yes**
Additional Notes					CMP Enrollment Configuration must allow Attributes via CO Enrollment Flow. Additionally, no CO Person or CO Person Role attributes may be defined.

⚠ For Self-Signup enrollments, you will need to somehow provide the URL to start the enrollment to potential enrollees, perhaps by sending it in email or posting it on a web page. To obtain the URL as an administrator, go to *People* >> *Enroll* to generate a list of available enrollment flows and copy the link from the appropriate *Begin* button.