Registry Enrollment (Rev 1, Registry 0.9.3 and earlier)

This page provides a detailed explanation of Registry Enrollment for versions up to (and including) v0.9.3. For information on Registry Enrollment in newer versions, see Registry Enrollment (Rev 2, Registry 0.9.4 and later). For information on configuring enrollment, see Registry Enrollment Flow Configuration.

By default, COmanage Registry uses an invitation based enrollment flow.

However, COmanage Registry Enrollment can be customized. It is controlled by two configurations:

- CMP Enrollment Configuration manages platform-wide (ie: across all COs managed by a given COmanage Registry installation) enrollment configuration, generally related to the process of making Organizational Identities, which must be consistent across the platform (it would be remarkably confusing to have per-CO configurations for organizational identity), known to the COmanage Registry. Only the CMP Administrators can adjust the CMP Enrollment Configuration.
- CO Enrollment Flows manage CO-level enrollment configuration, and are constrained by the CMP Enrollment Configuration. A CO can have more than one Enrollment Flow active at any given time.

See also the Registry Data Model overview.

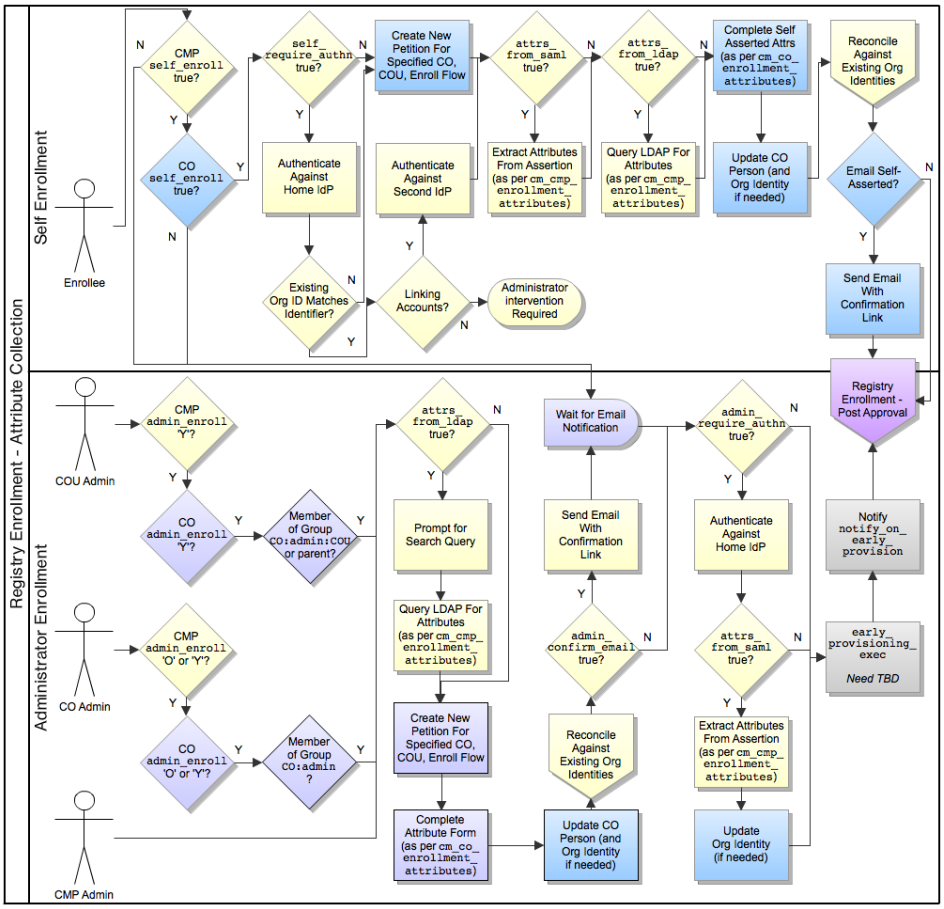
The Enrollment process is initiated by creating a Petition attached to an Enrollment Flow.

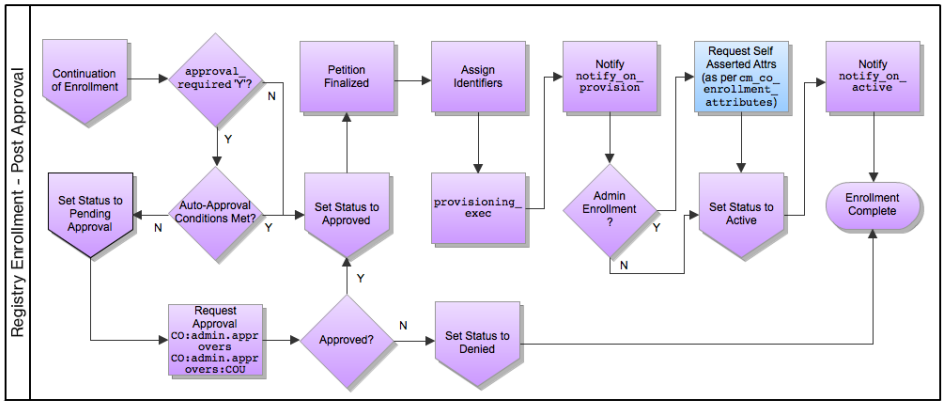
The Registry Enrollment is configurable, as described in this diagram and configured via cm_cmp_enrollment_configurations and cm_co_enrollment_flows:

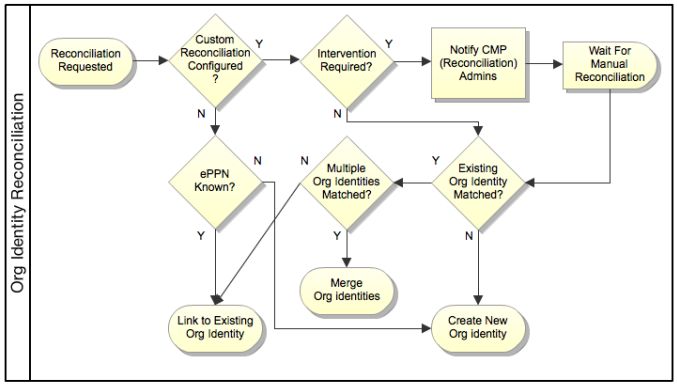
- Both LDAP and SAML may be in use simultaneously since different organizational sources may support different methodologies.
- Any attribute configured to be provided via LDAP or SAML becomes organizational-authoritative and cannot be changed by the enrollee. (This is currently true across all organizations, but this restriction may be removed in a future release.)

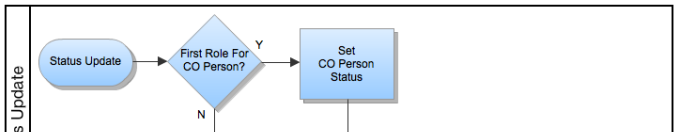
The Registry Enrollment model is designed to support the following:

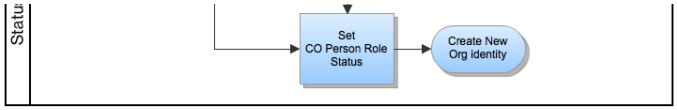
- Federated Identity: Authentication happens at a home institution's IdP. Attributes may or may not be retrieved. `self_require_authn` or `admin_require_authn` must be enabled.
- IdP of Last Resort: The CO will manage the user's credentials. `self_require_authn` or `admin_require_authn` may both be disabled. The early provisioning step is intended to support this model – allowing the creation of credentials before the user authentication step.
- Account Linking: An individual known to the platform has more than one IdP, and would like the identities asserted from each IdP linked to the same profile.


Registry Enrollment - Attribute Collection
Self Enrollment
Enrollee
CMP self_enroll true?
CO self_enroll true?
self_ require_authn true?
Authenticate Against Home IdP
Existing Org ID Matches Identifier?
Create New Petition For Specified CO, COU, Enroll Flow
Authenticate Against Second IdP
Linking Accounts?
Administrator intervention Required
attrs_ from_saml true?
Extract Attributes From Assertion (as per cm_cmp_ enrollment_ attributes)
attrs_ from_ldap true?
Query LDAP For Attributes (as per cm_cmp_ enrollment_ attributes)
Complete Self Asserted Attrs (as per cm_co_ enrollment_ attributes)
Update CO Person (and Org Identity if needed)
Reconcile Against Existing Org Identities
Email Self-Asserted?
Send Email With Confirmation Link
Registry Enrollment - Post Approval
Administrator Enrollment
COU Admin
CMP admin_enroll 'Y'?
CO admin_enroll 'Y'?
Member of Group CO:admin:COU or parent?
CO Admin
CMP admin_enroll 'O' or 'Y'?
CO admin_enroll 'O' or 'Y'?
Member of Group CO:admin ?
CMP Admin
attrs_ from_ldap true?
Prompt for Search Query
Query LDAP For Attributes (as per cm_cmp_ enrollment_ attributes)
Create New Petition For Specified CO, COU, Enroll Flow
Complete Attribute Form (as per cm_co_ enrollment_ attributes)
Wait for Email Notification
Send Email With Confirmation Link
admin_ confirm_email true?
Reconcile Against Existing Org Identities
Update CO Person (and Org Identity if needed)
admin_ require_authn true?
Authenticate Against Home IdP
attrs_ from_saml true?
Extract Attributes From Assertion (as per cm_cmp_ enrollment_ attributes)
Update Org Identity (if needed)
Notify notify_on_ early_ provision
early_ provisioning_ exec Need TBD


Registry Enrollment - Post Approval
Continuation of Enrollment
approval_ required 'Y'?
Set Status to Pending Approval
Auto-Approval Conditions Met?
Request Approval CO:admin.appr overs CO:admin.appr overs:COU
Approved?
Set Status to Denied
Set Status to Approved
Petition Finalized
Assign Identifiers
provisioning_ exec
Notify notify_on_ provision
Admin Enrollment ?
Request Self Asserted Attrs (as per cm_co_ enrollment_ attributes)
Set Status to Active
Notify notify_on_ active
Enrollment Complete


Org Identity Reconciliation
Reconciliation Requested
Custom Reconciliation Configured ?
Intervention Required?
Notify CMP (Reconciliation) Admins
Wait For Manual Reconciliation
ePPN Known?
Multiple Org Identities Matched?
Existing Org Identity Matched?
Merge Org Identities
Link to Existing Org Identity
Create New Org Identity


Status Update
First Role For CO Person?
Set CO Person Status


Set
CO Person Role
Status
Create New
Org identity