## 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.



