

Sponsors and Managers

- [Sponsors](#)
 - [Privacy Considerations During Enrollment](#)
 - [Sponsor Renewals](#)
- [Managers](#)
 - [Privacy Considerations During Enrollment](#)

Sponsors

Each [CO Person Role](#) can have a *sponsor* attached to it. The sponsor can be selected via an Enrollment Flow Attribute, or subsequently by manually editing the record.

The pool of eligible sponsors can be configured via *CO Settings* as follows:

- CO Administrators
- CO and COU Administrators
- Members of a specified CO Group
- Any Active CO Person

The sponsors capability may also be disabled. This may be advisable for deployments with large user populations, as disabling sponsors will reduce some database querying.

If a sponsor subsequently becomes ineligible to be a sponsor, they will remain as sponsors for any existing records. However, they may not become sponsors of new records, and any existing record must specify a new sponsor if edited.

Sponsor status may also be used in [Expiration Policies](#). Note that expiration policies apply to the status of the sponsoring CO Person (ie: whether or not the CO Person is *valid*) and not to whether or not the CO Person is *eligible* to be a sponsor ([CO-1140](#)).

As of Registry v3.3.0, Sponsor selection uses a "search while you type" people picker when more than 50 potential sponsors are available. The people picker supports search by partial name or complete email address or identifier. ⚠ This service may be disabled by default for some Enrollment Flow configurations. See *Privacy Considerations During Enrollment*, below.

As of Registry v3.3.0, if a Sponsor attribute is defined in an [Enrollment Flow](#), the Petitioner will be set as the default Sponsor when the following conditions are met:

1. There is no default Sponsor set in the Enrollment Attribute
2. The Enrollment Attribute is *Required*
3. The Petitioner is eligible to be a Sponsor, as per the CO Setting described above
 - a. This implies the Petitioner is a valid CO Person within the target CO

Privacy Considerations During Enrollment

When Sponsor selection is enabled during enrollment, consideration should be given to potential information release, in particular during anonymous or authenticated Enrollment Flows (*Petitioner Enrollment Authorization* is set to *None* or *Unauthenticated User*) where the Sponsor field is modifiable. In order for the Sponsor to be selectable, the Petitioner must be able to view available Sponsors. This effectively means any unregistered user can determine who the possible Sponsors are, and if any CO Person is a possible Sponsor, then the unregistered user can view all (active) members of the CO.

For smaller sets of possible Sponsors (less than 50), the entire set of Sponsors will be embedded in the Petition *petitioner_attributes* form as an HTML select. Anyone with a web browser will be able to easily view the list of Sponsors.

For larger sets, a people picker will be rendered instead of a select list. While this will no longer incorporate the full set of sponsors in the page source, for the people picker to work an API must be enabled to provide responses to search-while-you-type queries. This API requires authentication, however for anonymous or authenticated Enrollment Flows, the authenticator is simply the petitioner token, which effectively makes the API open to the world. As such, the API is *disabled* in this context by default. To enable the API for unregistered enrollments, tick *Enable People Picker for Self Service* in the Enrollment Flow configuration.

Possible mitigations for this exposure include:

- Reducing the set of available Sponsors
- Not permitting the selection of Sponsors for anonymous or authenticated Enrollment Flows
- Using a non-modifiable Sponsor for anonymous or authenticated Enrollment Flows
- None, if the people data is already public, for example via an organizational directory

Sponsor Renewals

As of Registry v4.1.0, a Sponsor may manage renewals of their Sponsored Roles using the [Sponsor Manager Plugin](#).

Managers

As of Registry v4.1.0, each [CO Person Role](#) can have a *manager* attached to it as well. The managers can be selected via an Enrollment Flow Attribute, or subsequently by manually editing the record.

All CO People are eligible to be Managers, and a CO Person can be their own Manager. Each CO Person Role can have at most one Manager, so dual reports cannot be directly reflected using this mechanism.

Unlike Sponsors, Managers have no semantic value to Registry. They cannot be used with Expiration Policies, and the pool of available Managers cannot be constrained.

Privacy Considerations During Enrollment

Manager selection during enrollment is subject to substantially similar considerations as for Sponsors. However, the people picker is always used (and therefore subject to the same *Enable People Picker for Self Service* configuration).