Consuming External Attributes via Web Server Environment Variables

A typical deployment pattern includes the collection of authoritative attributes provided from an external source, typically via a SAML or OIDC assertion, which are then passed to Registry via web server environment variables. This document describes best practices for collecting and managing attributes via this mechanism.

ⓘ The supported approaches for the collection of authoritative attributes via environment variables have been changed in Registry v3.1.0. The newer mechanisms provide a clearer separation between authoritative attributes and CO attributes. The older mechanisms are considered deprecated, and will be removed in Registry v5.0.0 (CO-1545).

ⓘ Attributes can also be collected from authoritative sources via other mechanisms, via Organizational Identity Sources.

Using EnvSource To Create Organizational Identities

Registry v3.1.0 introduces the EnvSource Organizational Identity Source plugin, which can be used to create Organizational Identities based on the attributes provided in web server environment variables. Typical uses of this plugin would be as part of a self sign-up enrollment flow, or as part of a self-service account linking enrollment flow.

⚠ Organizational Identities require a Primary Name. As such, EnvSource must be able to retrieve name values from the environment (ie: the remote identity provider must assert name attributes) in order to create an Organizational Identity. (Otherwise an error about "Save Associated" will be generated.)

⚠ The Enrollment Flow *Duplicate Enrollment Mode* configuration is not supported when using Enrollment Sources. However, as of Registry v4.1.0 EnvSource supports a plugin specific duplicate handing mode.

Self Signup

A self sign-up enrollment flow can be used for a new participant who has not yet joined the platform. This configuration will create a new Organizational Identity based on the attributes received via the environment variables, and a new CO Person record attached to the Organizational Identity, using attributes provided by the enrollee. (But see also Populating Default Values During Enrollment, below.) The enrollee will be able to log into the platform using the login identifier registered with the Organizational Identity.

1. Configure the EnvSource plugin, if not already done. (If you are reusing an existing plugin configuration, make sure it has exactly the same settings as below. If it does not have exactly the same settings as below you may instead create and configure a second instance of the EnvSource plugin.)
   a. Prior to Registry v4.0.0, do *not* attach a Pipeline to the plugin. (Pipelines are supported in Registry v4.0.0 and later.)
   b. Set Sync Mode to *Manual*.
   c. Enable Sync on Login, if appropriate.
   d. In the attribute configuration, flag at least one identifier type as *Login*.
2. Create a new Enrollment Flow with the following settings:
   a. Status: Active
   b. Petitioner Enrollment Authorization: Authenticated User
   c. Pipeline: None
   d. Identity Matching: None
   e. Require Approval: Optional
   f. Email Confirmation Mode: Optional
      i. ⚠ Email confirmation requires v3.3.0 or later
3. Add CO Person and CO Person Role attributes as appropriate. Do *not* add any Organizational Identity attributes.
4. From the Enrollment Flow configuration page, click *Attach Org Identity Sources*.
5. Click ⊕ *Add Enrollment Source.*
   a. Organizational Identity Source: Select the Env Source you previously configured
   b. Org Identity Mode: Authenticate

i. ℹ As of Registry v4.1.0, *Identify* mode is also supported for Org Identity Sources in a Self Signup flow. This is particularly useful if a Pipeline is attached to EnvSource, as it will defer CO Person creation or linking until after any enrollment attributes are collected.

Invitation (Registry v4.1.0 and later)

An invitation enrollment flow can be used for a new participant who has not yet joined the platform. Unlike the earlier configuration, this version will only create one Organizational Identity (via EnvSource). The enrollee will be able to log into the platform using the login identifier registered with the Organizational Identity based on the environment variables.

1. Configure the EnvSource plugin, if not already done. (If you are reusing an existing plugin configuration, make sure it has exactly the same settings as below.)
    a. Set Sync Mode to *Manual*.
    b. Enable Sync on Login, if appropriate.
    c. In the attribute configuration, flag at least one identifier type as *Login*.
2. Create a new Enrollment Flow with the following settings:
    a. Status: Active
    b. Petitioner Enrollment Authorization: CO Admin, COU Admin, CO or COU Admin, or another suitably restricted setting
    c. Identity Matching: None or Advisory
    d. Require Approval: Optional
    e. Email Confirmation Mode: Automatic or Review
    f. Require Enrollee Authentication: No
3. Add CO Person and CO Person Role attributes as appropriate.
    a. Do *not* add any Org Identity Attributes.
    b. An Email Address must be collected for email confirmation, and also to deliver the Invitation.
4. From the Enrollment Flow configuration page, click *Attach Org Identity Sources*.
5. Click ⊕ *Add Enrollment Source.*
    a. Organizational Identity Source: Select the Env Source you previously configured
    b. Org Identity Mode: Identify

Invitation (Registry v3.1.0 through v4.0.2)

An invitation enrollment flow can be used for a new participant who has not yet joined the platform. This configuration will currently create *two* new Organizational Identities (CO-1578), one to send the invitation and one based on the attributes received via the environment variables. A new CO Person record will be created attached to both Organizational Identities, using attributes provided by the enrollee. (But see also Populating Default Values During Enrollment, below.) The enrollee will be able to log into the platform using the login identifier registered with the Organizational Identity based on the environment variables.

1. Configure the EnvSource plugin, if not already done. (If you are reusing an existing plugin configuration, make sure it has exactly the same settings as below.)
    a. Prior to Registry v4.0.0, do *not* attach a Pipeline to the plugin. (Pipelines are supported in Registry v4.0.0 and later.)
    b. Set Sync Mode to *Manual*.
    c. Enable Sync on Login, if appropriate.
    d. In the attribute configuration, flag at least one identifier type as *Login*.
2. Create a new Enrollment Flow with the following settings:
    a. Status: Active
    b. Petitioner Enrollment Authorization: CO Admin, COU Admin, CO or COU Admin, or another suitably restricted setting
    c. Pipeline: None
    d. Identity Matching: None or Advisory
    e. Require Approval: Optional
    f. Email Confirmation Mode: Automatic or Review
    g. Require Enrollee Authentication: Yes
3. Add CO Person and CO Person Role attributes as appropriate. Add at least a minimal set of Organizational Identity attributes (Official Name and Email, both of which can be copied to CO Person).
4. From the Enrollment Flow configuration page, click *Attach Org Identity Sources*.
5. Click ⊕ *Add Enrollment Source.*
    a. Organizational Identity Source: Select the Env Source you previously configured
    b. Org Identity Mode: Identify

Account Linking

An account linking enrollment flow can be used for a participant with an existing CO Person record who wishes to add a new Organizational Identity, typically to authenticate using a different identity.

1. Configure the EnvSource plugin, if not already done. The same EnvSource used for Self Signup can be attached here as well. (If you are reusing an existing plugin configuration, make sure it has exactly the same settings as below.)
    a. Prior to Registry v4.0.0, do *not* attach a Pipeline to the plugin. (Pipelines are supported in Registry v4.0.0 and later.)
    b. Set Sync Mode to Manual.
    c. Enable Sync on Login, if appropriate.
    d. In the attribute configuration, flag at least one identifier type as *Login*.
2. Create a new Enrollment Flow with the following settings:
    a. Status: Active
    b. Petitioner Enrollment Authorization: CO Person
    c. Pipeline: None
    d. Identity Matching: Self
    e. Require Approval: No (unticked)

    f. Email Confirmation Mode: None
3. Do not add any Enrollment Attributes. (You will be asked to add one by default, simply page back or follow the breadcrumbs to skip it.)
4. From the Enrollment Flow configuration page, click *Attach Org Identity Sources*.
5. Click ⊕ *Add Enrollment Source*.
    a. Organizational Identity Source: Select the Env Source you previously configured
    b. Org Identity Mode: Authenticate
6. Apache Configuration required

Apache Configuration

```
RewriteEngine On
RewriteCond %{QUERY_STRING} !after_redirect
RewriteRule ^/registry/auth/logout.* https://%{SERVER_NAME}/registry/Shibboleth.sso/Logout?return=https://%
{SERVER_NAME}/registry/auth/logout/?after_redirect [L,R]
```

Populating Default Values During Enrollment

EnvSource is used to populate Organizational Identities. While a pipeline could be used to create a CO person record from this organizational identity, this is not typically recommended as external identity providers usually do not release sufficient attributes to create a full CO Person record. More typically, enrollment attributes are configured to present a form to the enrollee, for purposes of collecting additional attributes.

Attributes from environment variables can be used to pre-populate the enrollment attributes, reducing the amount of typing necessary. These attributes become the default values for the CO Person record, but can be changed by the petitioner. To configure this, simply set the appropriate environmental variable name in the *Environment Variable For Default Value* configuration for each Enrollment Attribute.

This mechanism is completely unrelated to EnvSource.

> Note that names are treated specially, since they have multiple components. The specified variable will be appended with `_HONORIFIC`, `_GIVEN`, `_MIDDLE`, `_FAMILY`, or `_SUFFIX` to generate the variable name for the appropriate component. For example, if the variable name `ENV_OIS_NAME` is specified, `ENV_OIS_NAME_GIVEN` will be used for the first/given name.
>
> See Managing Apache Web Server Environment Variables for hints on setting environment variable with commonly deployed authentication modules.

> Hidden variables cannot be given default values from environment variables.

> As of Registry v4.0.0, the IdentifierEnroller Plugin offers a similar capability.

CMP Enrollment Attributes

Prior to Registry v3.1.0, CMP Enrollment Attributes were used to provide this capability. See Registry Platform Configuration for more information. This functionality is scheduled for removal in Registry v5.0.0 (CO-1545).

In general, this older capability should not be used with the newer capabilities described above. However, if both are configured the newer capability will take precedence.

Email Confirmation and Authentication

If only the authenticated identifier is desired, *Email Confirmation and Authentication* can be used to collect it, and attach it to an Organizational Identity created by the Enrollment Flow. See the Enrollment Flow documentation for more information. This functionality is deprecated and scheduled for removal in v5.0.0.