Upgrading Registry to v3.2.0

CO Group Member Validity Dates

Registry v3.2.0 adds support for valid from and valid through dates for CO Group Memberships. To make full use of these, it will likely be necessary to run the `groupvalidity` Registry Job Shell.

Organizational Identity Source Plugin resultToGroups() Result Change

For custom Organizational Identity Source Plugins that implement `resultToGroup()`, the return value has changed. See Groupable Attributes for more details.

SalesforceSource Configuration Changes

Registry v3.2.0 changes how server configuration for the Salesforce Source plugin is managed. This change allows multiple plugins to share the same configuration. To update an existing configuration:

1. Add a new Server, via *Servers* > *Add a New Server*
    a. Set the server type to *OAuth2*.
    b. After the configuration has been saved, a Redirect URI will be available via the server configuration page. Keep this handy for the next step.
2. Login to Salesforce and edit the existing configuration for the connected app. Change the Callback URL to the one provided in the OAuth2 server configuration from the previous step.
    a. ⚠ It may take several minutes for the new Salesforce configuration to take effect.
3. Return to the OAuth2 Server configuration and complete the configuration.
    a. *Server URL*: The base URL of your Salesforce instance with `/services/oauth2` appended, eg https://test.salesforce.com/services/oauth2
    b. *Client ID*: The Consumer Key obtained from the Salesforce connected app configuration.
    c. *Client Secret*: The Consumer Secret obtained from the Salesforce connected app configuration.
    d. *Access Token Grant Type*: Authorization Code
    e. *Scope*: (Leave blank)
    f. Click *Save*.
4. Return to the OAuth2 Server configuration to obtain an OAuth token.
    a. The configuration should indicate that the Access Token is "Not Set", and there should now be a button "Obtain New Token".
    b. Upon clicking that button, you will be taken to the Salesforce login page. Log in as a sufficiently authorized user.
    c. After successful login, you should be returned to the OAuth2 Server configuration page, and the Acess Token should now be "Set".
5. Finally, edit the existing Salesforce Source configuration. Select the server created in step 1 and click *Save*. You *must* click Save, even if looks like your server is already selected.

SalesforceSource Additional API Call

As of Registry v3.2.0, during a SalesforceSource `retrieve()` call, if an Account object is associated with the retrieved object, the Account object will also be retrieved. This consumes an additional API call.

OrcidSource Configuration Changes

Registry v3.2.0 changes how server configuration for the ORCID Source plugin is managed. This change allows multiple plugins to share the same configuration. To update an existing configuration:

1. Add a new Server, via *Servers* > *Add a New Server*
    a. Set the server type to *OAuth2*.
    b. After the configuration has been saved, a Redirect URI will be available via the server configuration page. Keep this handy for the next step.
2. Login to your ORCID developer tools and edit the existing Redirect URIs. Change the Redirect URI to the one provided in the OAuth2 server configuration from the previous step.
3. Return to the OAuth2 Server configuration and complete the configuration.
    a. *Server URL*: https://orcid.org/oauth
    b. *Client ID*: The Client ID provided by ORCID
    c. *Client Secret*: The Client Secret provided by ORCID
    d. *Access Token Grant Type*: Client Credentials
    e. *Scope*: /read-public

    f. Click *Save*.
4. Click *Obtain New Token*, and authenticate if necessary.
5. Edit the existing ORCID Source configuration.
    a. An Additional ORCID Redirect URI will be presented. Return to the ORCID developer tools and add this second Redirect URI.
        i. ℹ Both Redirect URIs are required for the ORCID Source Plugin to fully function.
    b. Select the server created in step 1 and click *Save*. You *must* click Save, even if looks like your server is already selected.

Plugin Menu Icons

Plugins that insert a menu into the `coconfig` context must now define an icon.

Accessing Enrollment Flows

As of Registry v3.2.0, the "Enroll" link to view available Enrollment Flows (and the entire "People" menu) is no longer visible to CO People who are not Administrators. Links to specific Enrollment Flows can be made available via the "My Identity" menu by setting the *Enable My Identity Shortcut* in the Enrollment Flow's configuration.

Petition Specific Redirect Target Base64 Encoding

Petition Specific Redirect Targets use Base64 encoding to avoid URL parsing errors. Registry v3.2.0 supports character substitution to avoid conflicting characters that may result from the Base64 operation, and any code that generates a `return` parameter for initiating an Enrollment Flow should be updated. See the documentation for more information.

Password Authenticator Plugin

The Password Authenticator Plugin adds support for two new hashing types (SSHA and Plaintext). The configuration must be re-saved, even if support for the new hashing types is not enabled.

1. *Configuration* > *Authenticators*
2. For each defined Password Authenticator, click *Configure*, then optionally enable the desired hashing types, then click *Save*, even if you made no changes to the configuration.

Note that new hashes will not be written until a given password is changed.