

# Configuring CManage Enrollment Flows

This page gives a short overview on CManage enrollment flows and how to configure the most used cases: invitation and self-signup. More detailed (technical) information on enrollment flows can be found at the CManage application documentation:

- Enable enrolment flows: [How to Configure Enrollment Flows](#)
- Configure an invitation flow: [How to Configure an Invitation Enrollment Flow](#)
- Configure a Self Signup Flow: [How to Configure a Self Signup Enrollment Flow](#)

- [Basic Idea](#)
- [Configuration](#)
- [Main Configuration Form](#)
- [Enrollment Attributes](#)
- [OrgIdentity Sources](#)

## Basic Idea

An enrollment flow allows a user (in CManage also known as a **COPerson**) to enroll into a CO or COU they were not a member of yet. Enrollment flows are not meant to administer group membership; group administrators (group owners) can do that directly through the Group interface of CManage. Group membership does not infer any special rights to members, whereas CO and COU membership allows access to specific services.

During the enrollment flow, the system makes a distinction between the petitioner and the enrollee. The **petitioner** is the person that started the enrollment flow and the **enrollee** is the subject of the flow. For self-signup enrollment flows, petitioners and enrollees are the same. For invitation flows, the petitioner is the person creating the invitation.

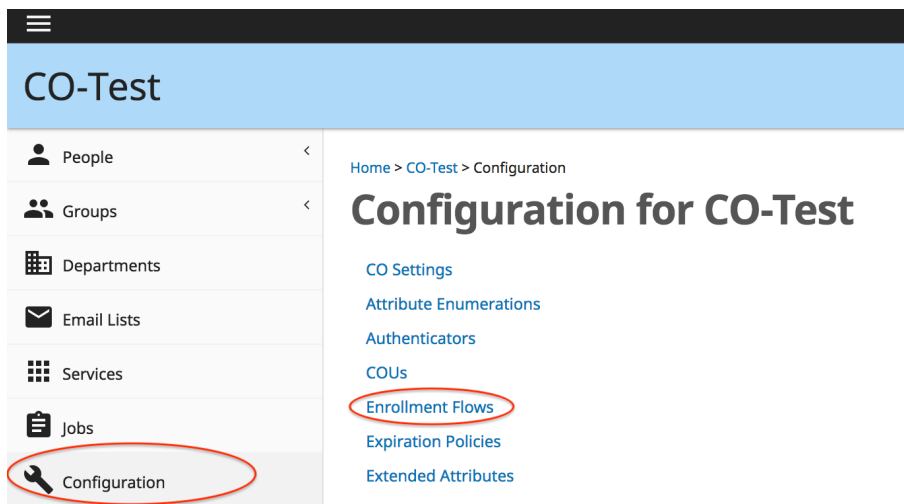
The basic steps of an enrollment flow are:

- creating the petition, entering the relevant values of the enrollee (think of name, email address, organization)
- confirming the email address, which sends an email to the enrollee
- viewing and accepting (confirming) the enrollment by the enrollee
- approving the enrollment by an administrator

Some of these steps are optional depending on the configuration of the enrollment flow.

## Configuration

Enrollment flows reside under the 'Configuration' form of a CO. Only CO administrators can configure these options, other users do not have this link.



New COs do not have any enrollment flows yet, but you can easily add or restore the default templates, which serve as a starting point for further configuration. Before configuring a new enrollment flow, you can duplicate a relevant template.

## Enrollment Flows

Name	Status	Petitioner Enrollment Authorization	Actions
Account Linking (Template)	Template	CO Person	<a href="#">Edit</a> <a href="#">Duplicate</a> <a href="#">Delete</a>
Additional Role (Template)	Template	CO or COU Admin	<a href="#">Edit</a> <a href="#">Duplicate</a> <a href="#">Delete</a>
Conscription With Approval (Template)	Template	CO or COU Admin	<a href="#">Edit</a> <a href="#">Duplicate</a> <a href="#">Delete</a>
Invitation	Active	None	<a href="#">Begin</a> <a href="#">Edit</a> <a href="#">Duplicate</a> <a href="#">Delete</a>
Invitation (Template)	Template	CO or COU Admin	<a href="#">Edit</a> <a href="#">Duplicate</a> <a href="#">Delete</a>
Self Signup With Approval	Active	None	<a href="#">Begin</a> <a href="#">Edit</a> <a href="#">Duplicate</a> <a href="#">Delete</a>
Self Signup With Approval (Template)	Template	None	<a href="#">Edit</a> <a href="#">Duplicate</a> <a href="#">Delete</a>

After this, the enrollment flow can be given a name and configured, which requires three steps:

- main configurations
- enrollment attributes
- org-identity-sources

These steps are described in more detail below.

## Main Configuration Form

A typical enrollment flow configuration form has the following options selected:

### Edit Invitation (Template)

Name	Invitation (Template)
Status *	Active
Petitioner Enrollment Authorization <small>Authorization required to execute this enrollment flow, see <a href="#">Enrollment Authorization</a> for details</small>	CO or COU Admin
Identity Matching <small>Identity Matching policy for this enrollment flow, see <a href="#">Identity Matching</a> for details</small>	None
Require Approval For Enrollment <small>If administrator approval is required, a Petition must be approved before the Enrollee becomes active.</small>	<input checked="" type="checkbox"/> Require Approval For Enrollment Approvers: <small>Members of this Group are authorized approvers (or else CO/COU admins by default)</small>
Email Confirmation Mode <small>See <a href="#">Email Verification</a> for mode definitions</small>	Review
Invitation Validity (Minutes) <small>When confirming an email address (done via an "invitation"), the length of time (in minutes) the confirmation link is valid for (default is 1 day = 1440 minutes)</small>	1440
Verification Email Message Template <small>Message template used for email sent as part of verification step</small>	<input checked="" type="checkbox"/>
Subject For Verification Email <small>Subject line for email message sent as part of verification step.</small>	Invitation to join (@CO_NAME)
Verification Email Body <small>Body for email message sent as part of verification step. Max 4000 characters.</small>	You have been invited to join (@CO_NAME). Please click the link below to accept or decline.  (@INVITE_URL)
Require Enrollee Authentication <small>Require enrollee to authenticate in order to complete their enrollment</small>	<input checked="" type="checkbox"/> Require Enrollee Authentication
Duplicate Enrollment Mode <small>How to handle automatically detected duplicate enrollments</small>	Create New Role If Different COU
From Address For Notifications <small>Email address notifications will come from</small>	

**Notification Group**  
Group to notify on new petitions and changes of petition status. (This is an informational notification. Separate notifications will be sent to approvers and enrollees, as appropriate.)

**Notify On Approved Status**  
Notify enrollee when Petition is approved  Notify On Approved Status

**Approval Email Message Template**  
Message template used for email sent as part of approval step

**Subject For Approval Email**  
Subject line for email message sent after Petition is approved. Petition to join (@CO\_NAME) has been approved

**Approval Email Body**  
Body for email message sent after Petition is approved. Max 4000 characters.  
Your petition to join (@CO\_NAME) as been approved. You may now log in to the platform.

**Notify on Finalization**  
Notify enrollee when Petition is finalized  Notify on Finalization

**Finalization Email Message Template**  
Message template used for email sent after finalization step

**Introduction**  
Optional text to display at the top of a Petition form

**Conclusion**  
Optional text to display at the bottom of a Petition form, before the Submit button

**Terms and Conditions Mode**  
How to handle Terms and Conditions at enrollment, if any are defined. See Terms and Conditions  Ignore

**Submission Redirect URL**  
URL to redirect to after Petition is submitted by someone who is not already in the CO.

**Confirmation Redirect URL**  
URL to redirect to after the email address associated with the Petition is confirmed. Leave blank for account linking enrollment.

**Finalization Redirect URL**  
URL to redirect to after processing of the enrollment has completed.

**Return URL Whitelist**  
Permitted regular expressions (one per line) for return parameter, which if specified overrides Finalization Redirect URL

**Theme**

[SAVE](#)

Important fields here are:

- **Petitioner Enrollment Authorization:** this defines who can start the enrollment. For invitation flows, you want this to be set to administrators of the CO or a relevant COU. For self-signup, you normally want this to be 'Authenticated Users'
- **Require Approval for Enrollment:** typically, this is checked to enable administrators to approve individual petitions, although you may want to uncheck this for invitation flows, where approval is done beforehand
- **Email Confirmation Mode:** this determines whether the enrollee can review their enrollment after clicking on the link in the confirmation email. If set to 'Automatic', enrollment proceeds immediately. 'Review' is a sensible setting.
- **Require Enrollee Authentication:** for invitation flows, you want the enrollee to authenticate after accepting the enrollment (review), so the system can gather the IdP provided attributes and this setting needs to be enabled ('on'). For self-signup flows where only authenticated users can enroll, authentication was already done at the start (and the IdP provided attributes were linked), so for self-signup this option can be unchecked ('off').

The other fields are either less relevant or very obvious and allow administrators to further personalize the enrollment experience.

## Enrollment Attributes

Enrollment attributes determine the attributes gathered of, from or by the enrollee during the enrollment flow:

Home > COmanage > Enrollment Flows > Edit Enrollment Flow

### Edit Invitation

[Edit Enrollment Attributes](#) [Duplicate](#) [Begin](#)

**Name**

A typical list of attributes looks as follows:

## Enrollment Attributes (Invitation)

[+ Add Enrollment Attribute](#) [+ Reorder Attributes](#)

Label	Attribute	▲ Order	Required	Actions
Name	Name (Official, Organizational Identity)	1	Required	<a href="#">Edit</a> <a href="#">Delete</a>
Email	Email (Official, Organizational Identity)	2	Required	<a href="#">Edit</a> <a href="#">Delete</a>
Affiliation	Affiliation (CO Person Role)	3	Required	<a href="#">Edit</a> <a href="#">Delete</a>
Organization	Organization (Organizational Identity)	4	Optional	<a href="#">Edit</a> <a href="#">Delete</a>
Title	Title (CO Person Role)	5	Optional	<a href="#">Edit</a> <a href="#">Delete</a>

Page 1 of 1, Viewing 1-5 of 5

This list determines which attributes are gathered and to which destination object the attributes are copied (note: **not from which source**). Administrators can determine which values are required, which fields are visible and which attributes can be further modified by the user:

- If using the SAMLSource OIS plugin (see below), the authoritative IdP attributes are stored non-modifiable in an attached Organisational Identity (OrgIdentity). It is therefore not essential that specific information needs to be non-modifiable to allow administrators to properly identify enrolled COPersons: administrators can always look at the related OrgIdentity with the relevant IdP attributes. This information is clearly visible when perusing an enrolled COPerson's data.
- The SAMLSource plugin tries to split a displayName field into givenName and familyName, but it uses a simple algorithm. Consider allowing users to modify their name to avoid cases where this automatic splitting fails, or where users have a different preferred name than their officially registered institute name. This opens the door for people that want to impersonate as someone else, but as mentioned above: administrators have easy access to the IdP provided attributes to correct such cases.
- The email address provided by the IdP might not be the preferred address for this specific CO of that COPerson, so consider allowing users to modify their email address. Alternatively, consider adding a hidden field for the official email address and a modifiable field for the preferred email address
- Please note that copying the IdP provided attributes without allowing users to modify (or even see) the values might violate the user consent and/or the institute privacy guidelines, depending on the scope of the CO and additional policies. In general, it is best practice to only filled required attributes using the IdP provided data as default, but allow users to modify their actual value before proceeding with enrollment.
- For invitation flow enrollment, the IdP attributes are not available yet when these attributes are gathered, so there is no way to copy IdP provided attributes.

Note: the following 3 attributes are REQUIRED for any invitation flow:

- Name
- Email
- Affiliation (CO Person Role)

COmanage will happily accept a flow without those attributes, but will then fail to submit the enrollment form with incomprehensible error messages like "Please check the highlighted field", while not of the fields are highlighted.

A typical attribute configuration form looks like this:

## Edit Name (Invitation)

<b>Label</b> <i>The label to be displayed when prompting for this attribute as part of the enrollment process</i>	<input type="text" value="Name"/>
<b>Description</b> <i>Descriptive text to be displayed when prompting for this attribute (like this text you're reading now)</i>	<input type="text"/>
<b>Attribute</b>	<input type="text" value="Name (Official, Organizational Identity)"/> <input type="text"/> <small>A name must consist of at least these fields:</small> <input type="text" value="Given Name"/> <input checked="" type="checkbox"/> Copy this attribute to the CO Person record
<b>Required</b>	<input type="text" value="Required"/>
<b>Ignore Authoritative Values</b> <i>Ignore authoritative values for this attribute, such as those provided via environment variables, SAML, or LDAP</i>	<input type="checkbox"/>
<b>Environment Variable For Default Value</b> <i>If populated, the value of this environment variable will be used as the default value for this attribute (See also <a href="#">this documentation</a>)</i>	<input type="text"/>
<b>Order</b> <i>The order in which this attribute will be presented (leave blank to append at the end of the current attributes)</i>	<input type="text" value="1"/>
<b>Default Value</b>	<input type="text"/>
<b>Modifiable</b> <i>If false, the Petitioner cannot change the default value placed into the Petition</i>	<input checked="" type="checkbox"/>
<b>Hidden</b> <i>If true, this field will not be rendered during enrollment</i>	<input type="checkbox"/>
<b>Take default from OrgIdentitySource</b> <i>If checked, try to find a default value on any attached OrgIdentitySource record for this petitioner if no default was found through environment values.</i>	<input checked="" type="checkbox"/>

Important fields on this form:

- The attribute you select is the attribute **to** which the gathered data is copied after completing the enrollment-step. For self-signup enrollments, the Organizational Identity attached to the enrollment is a non-modifiable IdP attribute related identity, so you should not select any attributes related to the Organizational Identity (as it cannot be overwritten). Doing so results in non-descriptive user-errors during enrollment.
- Some attributes are related directly to the COPerson (the identity of the user within the bounds of the CO). If a relevant attribute of the Organizational Identity is selected as attribute (in case of invite-flows), this form displays a 'Copy this attribute to the COPerson record' option, allowing you to match Organizational Identity and COPerson identity. This is specifically useful for attributes like name and email address. Note that this option is not available for all attributes, specifically the COPersonRole attributes (that determine the role this person is playing within the bounds of the CO or COU)
- The fields 'Ignore Authoritative Values' and 'Environment Variable for Default Value' can be left off and empty.
- The 'Take default from OrgIdentitySource' option determines if a 'relevant' attribute value is searched for in any attached OrgIdentity for the current enrollment. This matches for example 'preferred email' to 'preferred email', but if no 'preferred email' exists, it will take any email as default. Because of such cases, it is suggested to always allow users to review-and-modify the gathered attributes.
- The minimal required fields for names are either 'givenName' or 'givenName and familyName' and no other options can be configured.
- If you want users to enroll into a COU or sub-COU, you must add an attribute of type COU (COPersonRole), which allows you to specify the relevant COU. This attribute can be set hidden, non-modifiable, etc. as required. You can add a Group Membership attribute as well, through which you can enroll users directly into the relevant COU admin group to make them administrator. But in general, managing group membership is done elsewhere, in the CManage group interface. Promoting a COPerson to COU-administrator requires adding them to the relevant COU admin group and can be done outside any enrollment flow.

## OrgIdentity Sources

An OrgIdentity Source (OIS) is a data store that can supply relevant OrgIdentity attributes based on some common identifier. CManage typically uses email address as common identifier, which makes storing the right email address more of an issue.

CManage has a default OIS called 'EnvSource', which allows reading 'environment variables' of the webserver to scan for relevant authentication attributes introduced by back-end authentication systems like Shibboleth, auth\_mod\_mellon, etc. Because these variables are hidden from basic CO administrators and can differ based on the original IdP against which is authenticated, use of this specific OIS is not supported by SCZ.

Instead, SCZ supplies the SamlSource OIS. This OIS reads all relevant SAML attributes from the SCZ flow and creates a related, non-modifiable OrgIdentity record. To enable this OIS, you need to configure it under the CO configurations (ConfigurationOrganizational Identity Sources). The form looks as follows:

## Add a New Organizational Identity Source

Description *	<input type="text"/>
Plugin *	SamISource
Once a new Organizational Identity Source has been created, the Plugin cannot be changed	
Status *	Active
Sync Mode *	Manual
Do Not Query for Known Email Addresses	<input type="checkbox"/>
If an email address is already attached to an Org Identity associated with this Source, do not query for it	
Email Mismatch Mode	Create New Org Identity
If a returned record has a different email address than the one that was searched, how the record should be handled	
Sync on Login	<input type="checkbox"/>
If set, when a person logs into Registry and has a record from this source, the record will be resynced during the login process	
EPPN Identifier Type	
If set, use the identifier of this type to construct an ePPN	
EPPN Suffix	<input type="text"/>
If set, append this suffix to the EPPN Identifier to construct an ePPN (do not include @)	
Hash Source Records	<input type="checkbox"/>
Store a hashed version of the cached source record used by Registry to detect changes	

\* denotes required field

ADD

Important fields here:

- select the SamISource Plugin
- 'Sync Mode' should be 'Manual', because the SAML data is only available when the user logs in and hence cannot be synced when the user is offline
- 'Sync on Login' should be checked ('on')
- SamISource creates a login identifier based on different settings, so the 'EPPN' fields can be disregarded.
- Detecting changes does not cause any relevant behaviour, so hashing is not required

After completing this form, the SamISource plugin can be setup:

## Edit 1

Prefix* Defines the prefix used for SAML variables set in the environment	MELLON_
Identifier* Defines the identifier configured as REMOTE_USER for login	cmuid

\* denotes required field

SAVE

- The Prefix used is 'MELLON\_', without the quotes, but including the underscore
- The Identifier used by SCZ is called 'cmuid' (again, without the quotes)

With at least one OIS configured, a new option appears with the enrollment flow configuration screen:

## Edit Invitation

Name	Invitation	<a href="#">Edit Enrollment Attributes</a>	<a href="#">Attach Org Identity Sources</a>	<a href="#">Duplicate</a>	<a href="#">Begin</a>
Status *	Active				
Petitioner Enrollment Authorization	CO or COU Admin				
Authorization required to execute this enrollment flow, see Enrollment Authorization for details					
Identity Matching	None				

You can add several OIS-es, but the general case is to have only the SamISource OIS:

## Add a New Enrollment Source (Invitation)

<b>Organizational Identity Source*</b>	SamlSource ▾
<b>Org Identity Mode*</b> <small>Org Identity mode for this enrollment flow, see <a href="#">Organizational Identity Sources</a> for details</small>	Authenticate ▾
<b>Order</b> <small>The order in which this source will be queried, among all sources configured for this enrollment flow with this mode</small>	<input type="text"/> ↕

\* denotes required field

Depending on the type of flow, you will need to set the 'Org Identity Mode':

- for invitation flows, you need to set this to 'Identify', so you get an additional OrgIdentity record through which you can identify the enrolled COPerson afterwards
- for self-signup flows, you need to set this to 'Authenticate', so an OrgIdentity is created upon initial authentication, which can be used to set default values for enrollment attributes