



[www.egi.eu](http://www.egi.eu)

@EGI\_eInfra

## Authentication and Authorisation Infrastructure Training: Identity management with Check-in VO management with COmanage

Nicolas Liampotis (GRNET)

Nick Evangelou (GRNET)



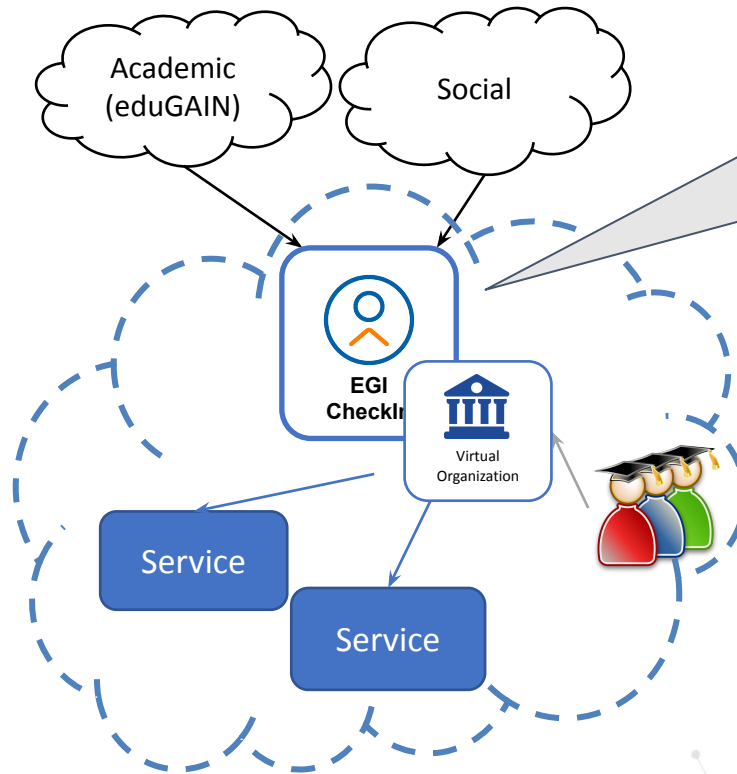
The work of the EGI Foundation  
is partly funded by the European Commission  
under H2020 Framework Programme

- Introduction
- User Identity Management with EGI Check-in
  - Sign-up
  - Profile view
  - Identity linking
- Virtual Organization (VO) Management with COmanage Registry
  - VO enrollment flows
  - VO group membership & role management
  - VO statistics
  - VO membership API
  - LDAP Access to VO membership information

# Authentication & Authorisation

*The big picture*

- HO User Identifier
- Name
- Email
- Affiliation
- Assurance



- Unique Check-in identifier → linked to one or more HO identities
- Assurance
- VO/group membership & roles
- Capabilities
- Site/service roles (GOCDDB)

HO	Home Organisation
VO	Virtual Organisation

# Authentication & Authorisation

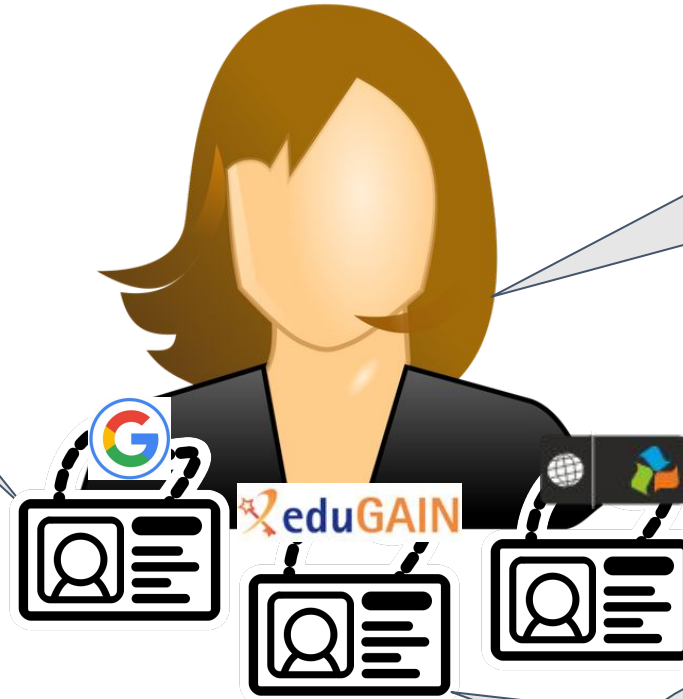
## *Identity attributes*

- HO User Identifier
- Name
- Email
- Affiliation
- Assurance

- Unique Check-in identifier → linked to one or more HO identities
- Assurance
- VO/group membership & roles
- Capabilities
- Site/service roles (GOCDDB)

- HO User Identifier
- Name
- Email
- Affiliation
- Assurance

- HO User Identifier
- Name
- Email
- Affiliation
- Assurance



HO Home Organisation

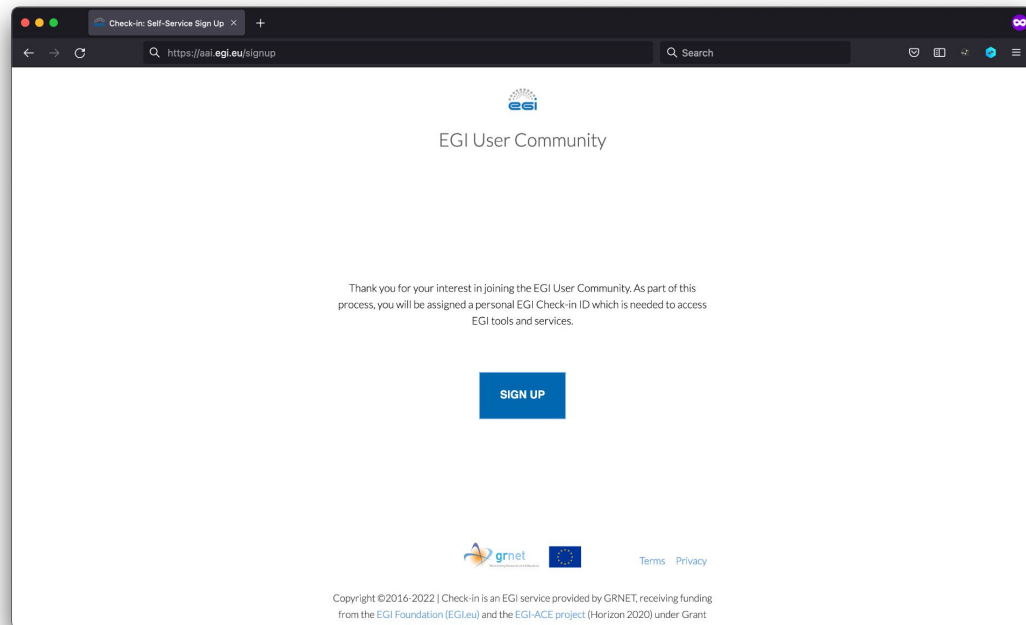
VO Virtual Organisation

# User Identity Management with EGI Check-in

Accessing resources protected by EGI Check-in requires signing up using your existing academic/social account

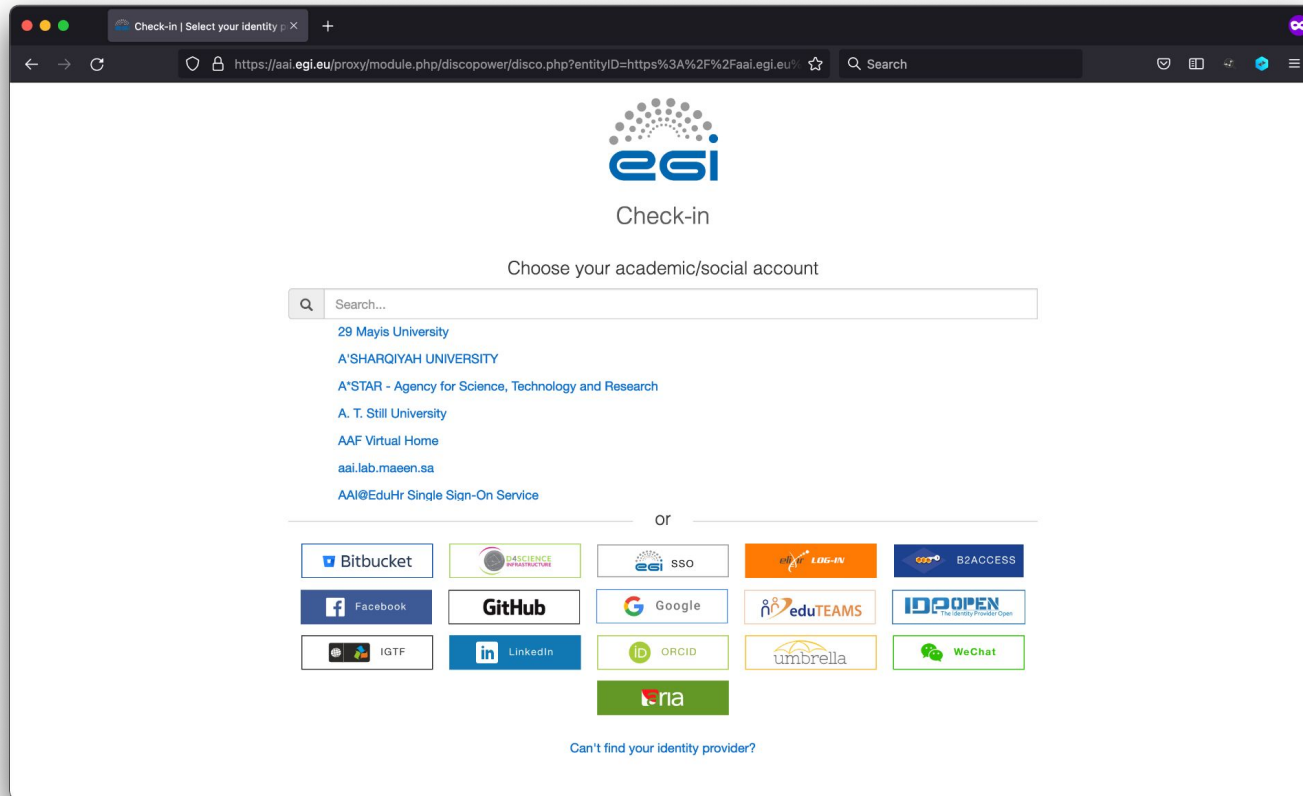
→ *Try me!*

<https://aai-demo.egi.eu/signup>



# User Sign-up | Login

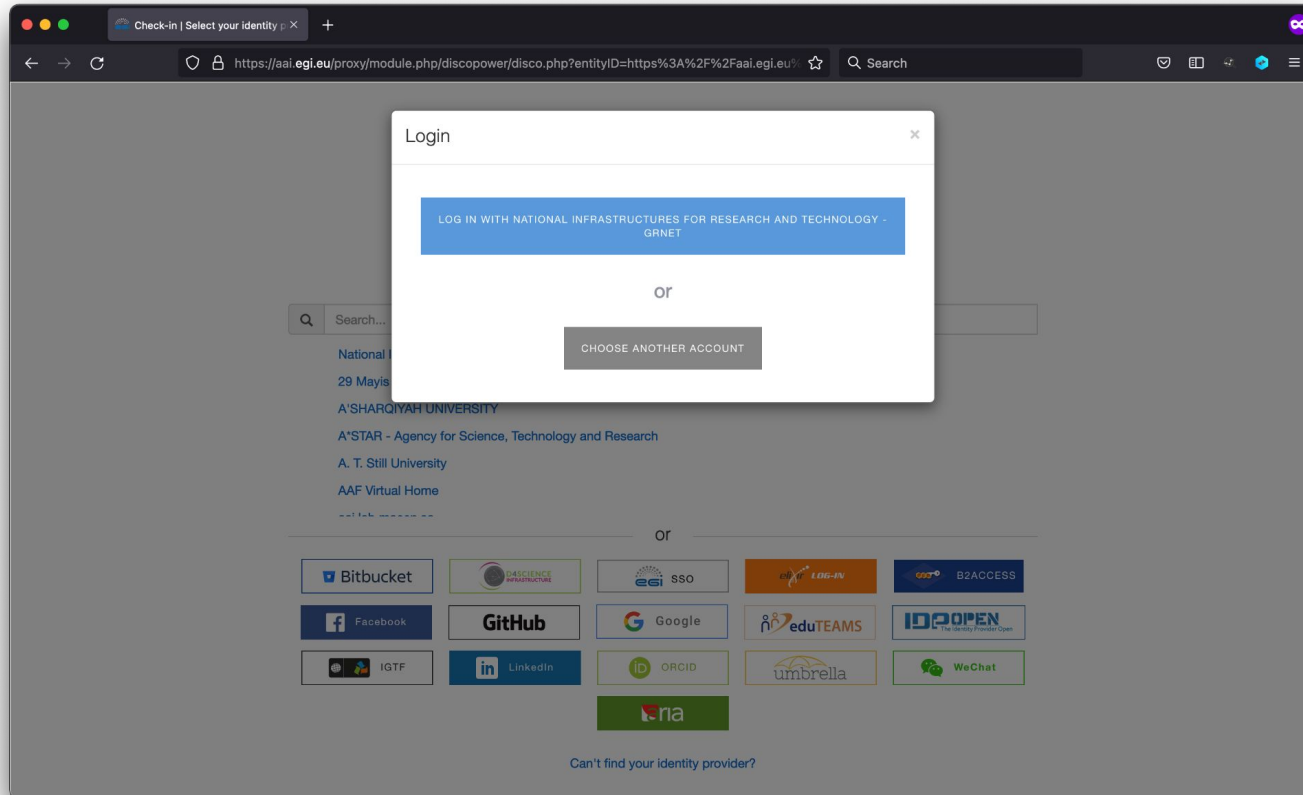
## Identity Provider Discovery



The screenshot shows a web browser window with the URL `https://aai.egi.eu/proxy/module.php/discopower/disco.php?entityID=https%3A%2F%2Faai.egi.eu%3A`. The page title is "Check-in | Select your identity". The main content area features the ESI logo and the heading "Check-in". Below this, the instruction "Choose your academic/social account" is displayed. A search bar with the placeholder "Search..." is present. The search results list several institutions: 29 Mayis University, A'SHARQIYAH UNIVERSITY, A\*STAR - Agency for Science, Technology and Research, A. T. Still University, AAF Virtual Home, aai.lab.maeen.sa, and AAI@EduHr Single Sign-On Service. Below the search results, the word "or" is centered. A grid of identity provider logos is shown, including Bitbucket, B2ACCESS, Facebook, GitHub, Google, eduTEAMS, ID OPEN, IGTF, LinkedIn, ORCID, umbrella, WeChat, and ria. At the bottom of the grid, there is a link that says "Can't find your identity provider?".

# User Login

## Identity Provider Discovery



The screenshot shows a web browser window with a URL: `https://aai.egi.eu/proxy/module.php/discopower/disco.php?entityID=https%3A%2F%2Faai.egi.eu%2F`. A modal window titled "Login" is displayed in the center. The modal contains a blue button with the text "LOG IN WITH NATIONAL INFRASTRUCTURES FOR RESEARCH AND TECHNOLOGY - GRNET". Below this button, the word "or" is centered. Underneath "or" is a grey button labeled "CHOOSE ANOTHER ACCOUNT".

In the background, a search bar is visible with the text "Search...". Below the search bar, a list of identity providers is shown, including: National I, 29 Mayıs, A'SHARQIYAH UNIVERSITY, A\*STAR - Agency for Science, Technology and Research, A. T. Still University, and AAF Virtual Home. Below this list, another "or" separator is present, followed by a grid of identity provider logos: Bitbucket, BASCIENCE, EGI SSO, UG-IV, B2ACCESS, Facebook, GitHub, Google, eduTEAMS, IDOPEN, IGTF, LinkedIn, ORCID, umbrella, WeChat, and ria. At the bottom of the modal, there is a link that says "Can't find your identity provider?".



## Step 1

Review user profile information

- name
- email
- affiliation

and agree to Acceptable Use Policy (AUP)

## Step 2

Verify email address - *only if a verified email address is not released by the user's authenticating identity provider*

## Access

Gain *authorised* access to resources

# User Sign-up

## Step 1 - Review

EGI ID  
Identifier  
1c96d5eccf1513b8fd9e0873a93a8998a4a3c572991b6b29aef1c

Name\*  
Your full name

Given Name\*  
Ioannis

Family Name\*  
Igoumenos

Email  
Your current email address

Email\*  
Ioigoume@gmail.com

- ✓ Review profile information
- ✓ Agree to AUP

EGI ID  
Identifier  
1c96d5eccf1513b8fd9e0873a93a8998a4a3c572991b6b29aef1c211a@egi.eu

Name\*  
Your full name

Given Name\*  
Ioannis

Family Name\*  
Igoumenos

Email  
Your current email address  
Ioigoume@gmail.com

Affiliation  
Faculty

Organisation  
Organisation\*

Agree to Acceptable Use Policy and Conditions of Use (AUP)  
You must review and agree to the following AUP before continuing.

EGI AUP Terms of Use  
 Review Acceptable Use Policy  Agree

After you click Submit, we'll send you an email and you simply click on a link to confirm your email address.

\*denotes required field

SUBMIT



Next, you will need to confirm your email address. Check your inbox and open the link on your browser.

This step is **SKIPPED** in case of an email known to be **verified** by the Identity Provider

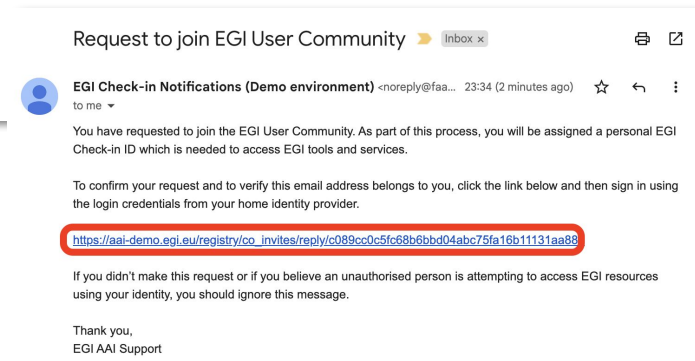


## We Sent You An Email

Just **click the link in that email** to complete your signup.

If you do not find the email in your Inbox, please check your **Spam** or **Junk** folder for an email from **EGI Check-in Notifications** ✉ noreply@faai.grnet.gr. If you do find the email in these folders, mark the email as "safe" or "not spam" to ensure that you receive any future notifications about your EGI Check-in ID.

YOU WILL HAVE **72 HOURS** TO VERIFY YOUR ACCOUNT




# User Sign-up

## Step 2 - Verify email

Click on “Accept” to finalise the registration.

This step is **SKIPPED** in case of an email known to be **verified** by the Identity Provider



EGI User Community

Invitation to EGI User Community

---


Invitation for IOANNIS IGOUMENOS ✔ Accept ✘ Decline

Click Accept to complete your registration		
EGI ID	Identifier	[Redacted]
Name* <i>Your full name</i>	Given Name	IOANNIS
	Family Name	IGOUMENOS
Email	Email	[Redacted]
Affiliation	Affiliation	Faculty
Organisation	Organisation	[Redacted]

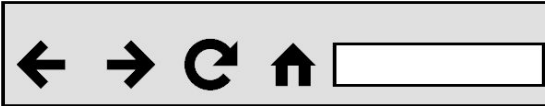
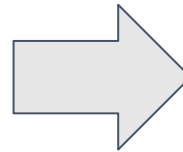
# User Sign-up

*Access resources*


Your enrollment is being processed,  
please do not refresh or close and click  
back button on this window.



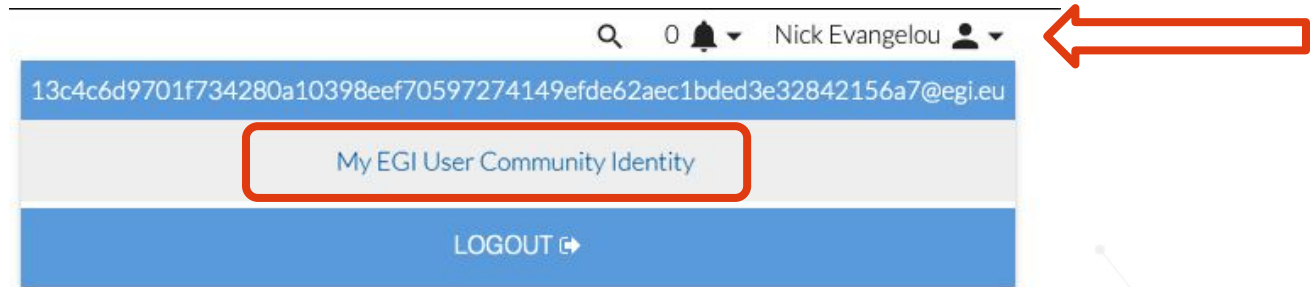
29%



**Welcome!**



1. Go to <https://aai.egi.eu/registry> (or <https://aai-demo.egi.eu/registry> for the DEMO environment)
2. Select **Login** and authenticate using any of the login credentials already linked to your Check-in profile
3. From the top bar menu, select **<Your name>** and click **My EGI User Community Identity**



Identity linking allows accessing resources with the same Check-in ID using different login credentials

1. Select **Actions** → **Link New Identity** from your Check-in Profile page

Organizational Identities					# Actions
Name	Source	Valid From (Europe/Berlin)	Valid Through (Europe/Berlin)	Login Identifiers	Link New Identity
Nicolas	https://aai- demo.egi.eu			4ced25112475ce6d75812efb2966fabf2-9910ff995ff914	



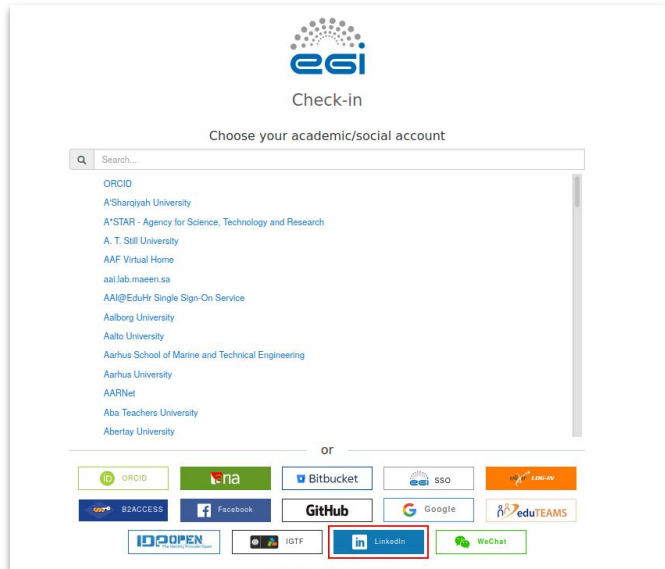
2. Click **Begin**

### Link New Identity

Identity linking allows you to access EGI resources with your existing EGI ID, using any of the login credentials you have linked to your account. Proceed to link a new identity to your EGI account.

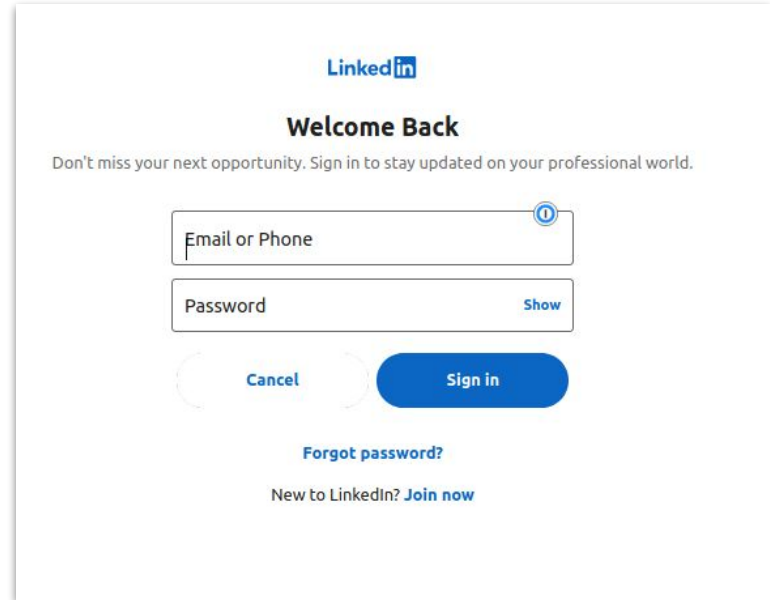
**BEGIN** →

### 3. Choose new Identity Provider from the list



**IMPORTANT: Select "CHOOSE ANOTHER ACCOUNT"**

### 4. Authenticate with the new Identity Provider





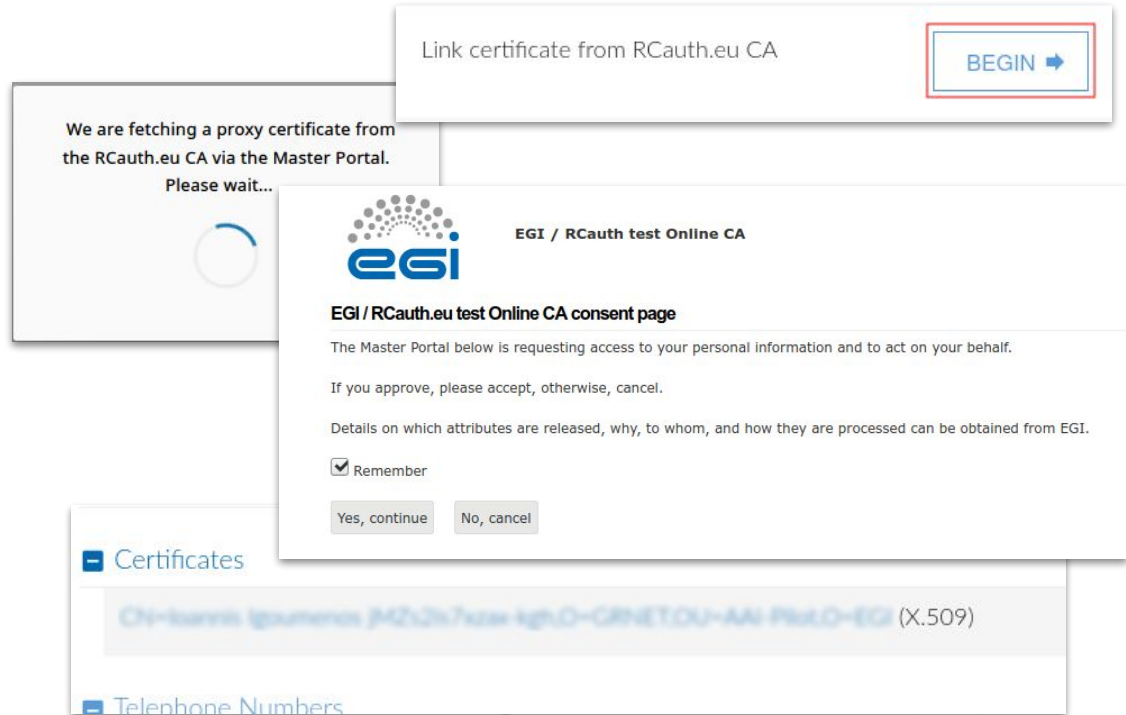
The new Identity is linked under your profile

SSH Keys Saved Add

Organizational Identities Link New Identity

Name	Source	Valid From (Europe/Helsinki)	Valid Through (Europe/Helsinki)	Login Identifiers
Ioannis Igoumenos (11820)	https://aai.egi.eu /orcid/saml2 /idp/metadata.php			ea394a6a26d631fb71246fe0062471100577179 (epuid)
IOANNIS IGOUMENOS (11822)	https://aai.egi.eu /linkedin/saml2 /idp/metadata.php			b53743953f6f24dd412ec0c82512dc9cbd1031a- (epuid)

Select **Actions** → **Link certificate from RCauth.eu CA**



The screenshot illustrates the process of linking a certificate from RCauth.eu CA. It features several overlapping windows:

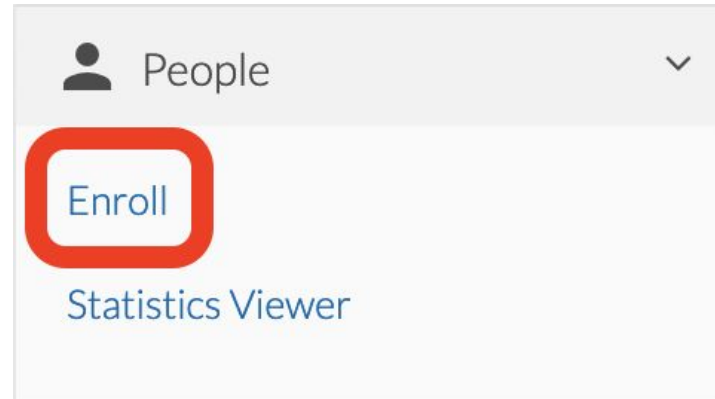
- Link certificate from RCauth.eu CA**: A window with a red-bordered **BEGIN** button.
- We are fetching a proxy certificate from the RCauth.eu CA via the Master Portal. Please wait...**: A window with a circular progress indicator.
- EGE / RCauth test Online CA**: A consent page with the EGI logo and the following text:
  - EGE / RCauth.eu test Online CA consent page**
  - The Master Portal below is requesting access to your personal information and to act on your behalf.
  - If you approve, please accept, otherwise, cancel.
  - Details on which attributes are released, why, to whom, and how they are processed can be obtained from EGI.
  - Remember
  - Yes, continue** **No, cancel**
- Certificates**: A window showing a list of certificates, with one entry highlighted: `01-barris igueneris J4ZL2h7zse 4ghD-GRNETOU-AAI Pk4D-EGE (X.509)`.
- Telephone Numbers**: A partially visible window at the bottom.

# VO Management with COnmanage Registry

# Requesting VO Membership

- User can request membership to a VO through an **enrollment flow**
- Each enrollment flow has a unique **URL** where the user can go to enroll to the desired VO
  - VO managers can share this URL to users, or
  - Users can click **Enroll** from the **People** menu and select the suitable enrollment flow

[https://aai.egi.eu/registry/co\\_petitions/start/coef:<##>](https://aai.egi.eu/registry/co_petitions/start/coef:<##>)



Click **Begin** to start the enrollment flow:

Home > EGI User Community > Join vo.example.eu

Join vo.example.eu

Thank you for your interest in participating in vo.example.eu VO. Please, note that you will not be able to use your EGI Check-in ID to access EGI resources until your request to join the community has been approved by an administrator.

BEGIN →

At the next page, click **Review Acceptable Use Policy** and check the **I Agree** box. Then, you can click “**SUBMIT**” to continue the enrollment flow.

Agree to Acceptable Use Policy and Conditions of Use (AUP)  
*You must review and agree to the following AUP before continuing.*

EXAMPLE TERMS AND CONDITIONS

Review Acceptable Use Policy  I Agree

When the petition is submitted, a message will be shown at the top of the screen:

A green rectangular message box with rounded corners and a white checkmark icon on the left. The text inside reads "Petition Submitted. Awaiting Review." in a dark green font.

✔ Petition Submitted. Awaiting Review.

Then a VO manager can approve or deny your request

# Managing VO Memberships

## *VO membership request notification*

Once a user submits a VO membership petition:

- all VO managers are notified with an email containing a link to the petition.
- they will receive a notification on their CManage profile. At the top right corner clicking the bell icon someone can see all the notifications.



Home > EGI User Community > Notifications > Notification

### Notification

<b>Comment</b>	Petition for Nikos Mastoris changed status from Created to Pending Approval (Join EXAMPLE Virtual Organisation)
<b>Status</b>	Pending Resolution <input type="button" value="Cancel"/>
<b>Source</b>	co_petitions
<b>Subject</b>	Nikos Mastoris
<b>Recipient</b>	CO:COU.vo.example.org.admins
<b>Actor</b>	Nikos Mastoris
<b>Action</b>	CPUP
<b>Created</b>	Mon Oct 25 11:54:16 2021 Europe/Helsinki
<b>Last Notification</b>	Mon Oct 25 11:54:18 2021 Europe/Helsinki
<b>Resolved</b>	
<b>Notification Email Subject</b>	Notification for "Join EXAMPLE Virtual Organisation" (EGI User Community)
<b>Notification Email Body</b>	Petition for Nikos Mastoris changed status from Created to Pending Approval (Join EXAMPLE Virtual Organisation) <a href="https://aai-dev.egi.eu/registry/co_petitions/view/12924">https://aai-dev.egi.eu/registry/co_petitions/view/12924</a>
<b>Resolution Email Subject</b>	
<b>Resolution Email Body</b>	

Clicking the petition URL either from the email you received or at the notification message, you can review the request.

# Managing VO Memberships

## VO membership request review

View Petition for [redacted]

### Petition

Status

Pending Approval

APPROVE

DENY

Optional

*If provided and the message template suitably configured, this comment will be made available to the enrollee. Use the "Add Comment" option instead for privileged comments that should not be visible to the enrollee.*

Enrollment Flow

Join vo.example.org VO

Enrollment Flow Next Step

waitForApproval

The VO Manager can provide justification of the approval or denial of the user's Petition

The Petition review page release information about the User's level of assurance.

### Attached Identities

CO Person

CO Person Role

43928

Organizational Identity

Organizational Identity Source  
Records

### Assurance

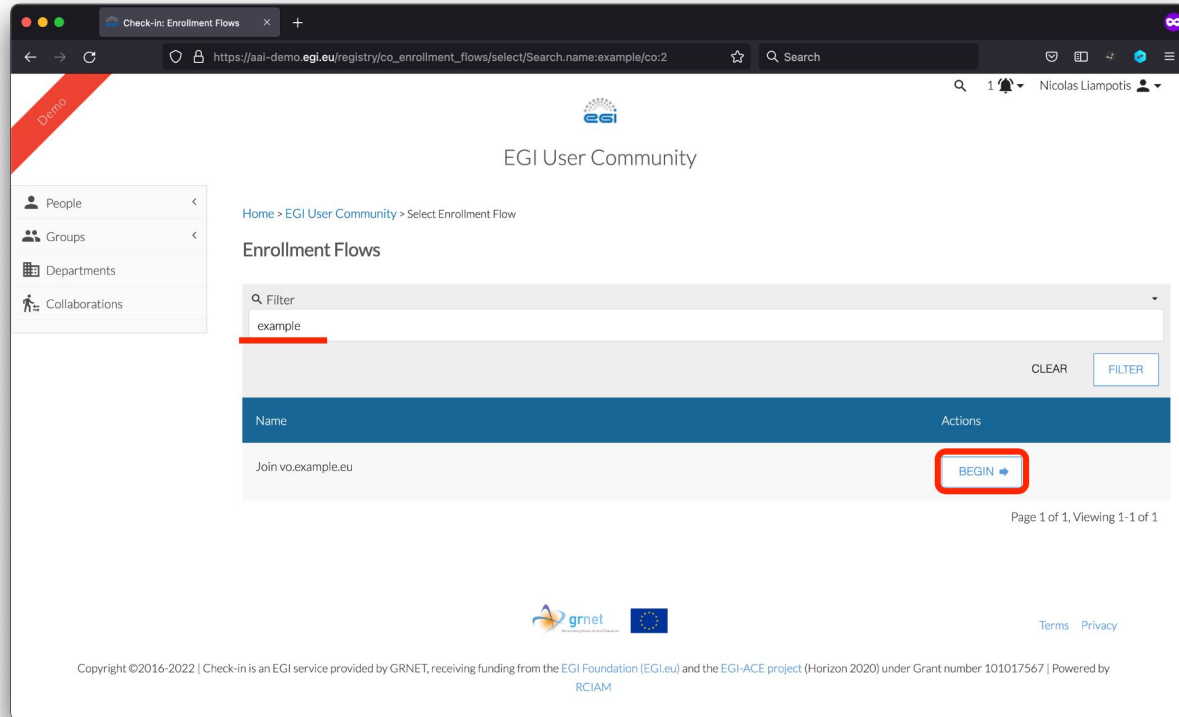
Organizational Identity  
(<https://janus.cnrs.fr/idp>)

<https://aai.egi.eu/LoA#Substantial> (profile)



# Requesting VO Membership

→ Try me!



[https://aai-demo.egi.eu/registry/co\\_petitions/start/coef:45](https://aai-demo.egi.eu/registry/co_petitions/start/coef:45)

# Using VO Membership for Authorization

*VO/Group membership and role information*

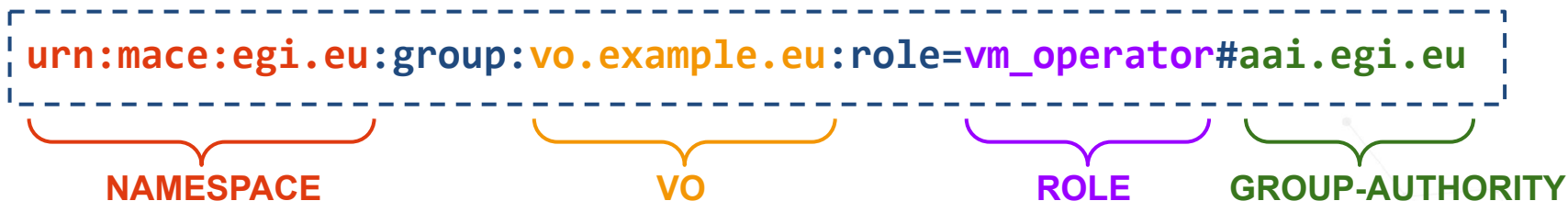
- Allows services to control access to resources based on information about the VO/groups a user is a member of
- One or more values encapsulated in:
  - `eduPersonEntitlement` attribute (SAML)
  - `eduperson_entitlement` claim (OIDC)
- Each value formatted as a URN → [AARC-G002](#)

```
<NAMESPACE>:group:<VO>[:<GROUP>*][:role=<ROLE>]#<GROUP-AUTHORITY>
```

# Using VO Membership for Authorization

*VO/Group membership and role information (Contd.)*

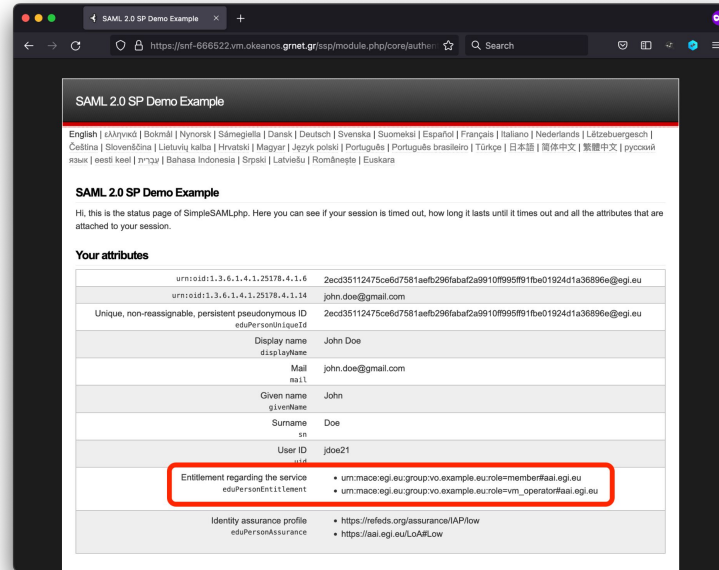
- Example values:



# Using VO Membership for Authorization

*VO/Group membership and role information (Contd.)*

→ Try me!



SAML 2.0 SP Demo Example

English | ελληνικά | Български | Nyorská | Sáimegiella | Dansk | Deutsch | Svenska | Suomi | Español | Français | Italiano | Nederlands | Lëtzebuergesch | Čeština | Slovenščina | Lietuvių kalba | Hrvatski | Magyar | Język polski | Português | Português brasileiro | Türkçe | 日本語 | 繁體中文 | 简体中文 | pyccckий язык | eesti keel | Bahasa Indonesia | Srpski | Latviešu | Românește | Euskara

**SAML 2.0 SP Demo Example**

Hi, this is the status page of SimpleSAML.php. Here you can see if your session is timed out, how long it lasts until it times out and all the attributes that are attached to your session.

**Your attributes**

urn:oid:1.3.6.1.4.1.25178.4.1.6	2ecc35112475ce6f7581aefb296fabaf2a9910f995f91fbc01924d1a36896e@egi.eu
urn:oid:1.3.6.1.4.1.25178.4.1.14	john.doe@gmail.com
Unique, non-reassignable, persistent pseudonymous ID eduPersonPersistentID	2ecc35112475ce6f7581aefb296fabaf2a9910f995f91fbc01924d1a36896e@egi.eu
Display name displayName	John Doe
Mail mail	john.doe@gmail.com
Given name givenName	John
Surname sn	Doe
User ID uid	jdoe21
Entitlement regarding the service eduPersonEntitlement	<ul style="list-style-type: none"> <li>urn:mace.egi.eu:group:vo.example.eu:role=member/aa.egi.eu</li> <li>urn:mace.egi.eu:group:vo.example.eu:role=vm_operator/aa.egi.eu</li> </ul>
Identity assurance profile eduPersonAssurance	<ul style="list-style-type: none"> <li>https://refeds.org/assurance/IAP/low</li> <li>https://aa.egi.eu/LOA/low</li> </ul>

<https://snf-666522.vm.oceanos.grnet.gr/ssp/module.php/core/authenticate.php?as=egi-demo-sp>

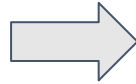
- VO groups in COmanage can only be created by Check-in platform administrators
- Contact [checkin-support@mailman.esi.eu](mailto:checkin-support@mailman.esi.eu) indicating the following information for every (sub)group:
  - VO name
  - Group name
  - Group description
  - Optional, Group manager(s)
  - Optional, Parent VO group name (in the case of a hierarchical group, e.g. <VO> → <PARENT\_GROUP> → <GROUP>)
- *Known limitation: Group names must be unique so the names may need to be adjusted to guarantee their uniqueness*

<https://docs.esi.eu/users/aai/check-in/vos/#managing-vo-groups>

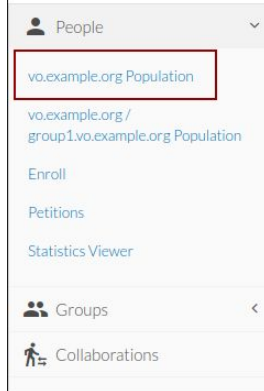
# Management of VO group members

## Adding member to VO group (1/2)

1) Expand the People drop down menu and click **<VO-NAME> Population** (for example, vo.example.org Population)



2) Find the user you want to add to the VO Group and click **Edit**.



### EGI User Community People

Toggle All: Open Closed Sort By: ▲ Name Status Created Modified

Filter

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	⌕
												▶ Petr Machacek (Petr.Machacek@cesnet.cz)	Active	<a href="#">Edit</a>												
												▶ Daniel Mallmann (d.mallmann@fz-juelich.de)	Active	<a href="#">Edit</a>												
												▶ Ricardo Martins (rjmartins@lnec.pt)	Active	<a href="#">Edit</a>												
												▶ Nick Mastoris (lonick85@hotmail.com)	Active	<a href="#">Edit</a>												
												▶ Nikos Mastoris (nmastoris@admin.grnet.gr)	Active	<a href="#">Edit</a>												
												▶ Nikos Mastoris (nmastoris@admin.grnet.gr)	Active	<a href="#">Edit</a>												
												▶ Emmanuel Medernach (emmanuel.medernach@iphc.cnrs.fr)	Active	<a href="#">Edit</a>												

# Management of VO group members

## Adding member to VO group (2/2)

3) Click Add at the Role Attributes section of the user profile



4) Fill in the fields in the form and click **Add**. The user now is a member of the new VO group.

### Role Attributes

COU	Title	Affiliation	Valid From	Valid Through	Status	Actions
vo.example.org		Member	2020-10-09 00:00:00	2021-10-08 23:59:59	Active	<div style="border: 1px solid #ccc; padding: 2px;"> <span style="border: 1px solid red; padding: 2px;">+ Add</span> </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> <span>Edit</span> </div> <div style="border: 1px solid #ccc; padding: 2px; margin-top: 2px;"> <span>Delete</span> </div>

Home > EGI User Community > My Population > Ioannis Igoumenos > Add CO Person Role

### Add a New CO Person Role (Ioannis Igoumenos)

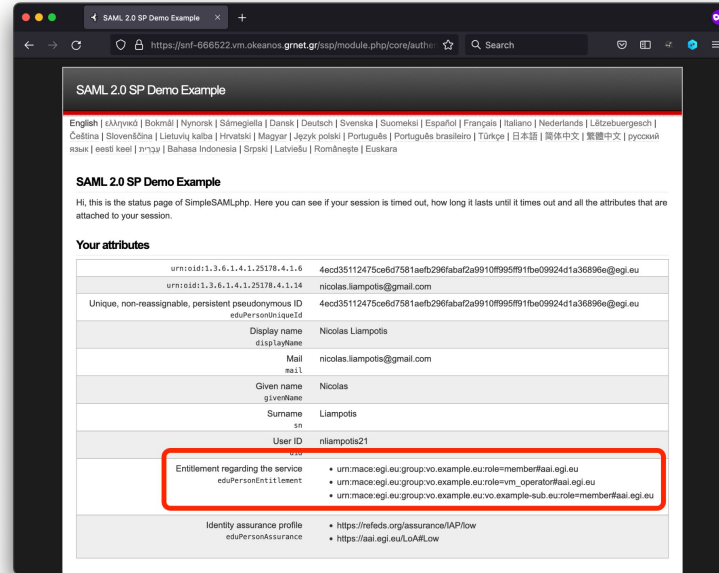
#### Role Attributes

EGI User Community COU	<input type="text" value="vo.example.org / group1.vo.example.org"/>
EGI User Community Affiliation *	<input type="text" value="Member"/>
Status *	<input type="text" value="Active"/>

# Using VO Membership for Authorization

## VO/Group membership and role information

→ Try me!



The screenshot shows a web browser window with the URL <https://snf-666522.vm.oceanos.grnet.gr/ssp/module.php/core/authenticate.php?as=egi-demo-sp>. The page title is "SAML 2.0 SP Demo Example". Below the title, there is a list of languages. The main content area is titled "SAML 2.0 SP Demo Example" and contains a message: "Hi, this is the status page of SimpleSAML.php. Here you can see if your session is timed out, how long it lasts until it times out and all the attributes that are attached to your session." Below this message is a section titled "Your attributes" which contains a table of attributes and their values. A red box highlights the "Entitlement regarding the service" attribute.

Attribute Name	Value
urn:oid:1.3.6.1.4.1.25178.4.1.6	4ecc35112475ce6d7581aefb296fabaf2a9910f995f91fbc09924d1a36896e@egi.eu
urn:oid:1.3.6.1.4.1.25178.4.1.14	nicolas.liampotis@gmail.com
Unique, non-reassignable, persistent pseudonymous ID	4ecc35112475ce6d7581aefb296fabaf2a9910f995f91fbc09924d1a36896e@egi.eu
eduPersonInLiquId	
Display name	Nicolas Liampotis
displayname	
Mail	nicolas.liampotis@gmail.com
mail	
Given name	Nicolas
givenName	
Surname	Liampotis
sn	
User ID	niampotis21
Entitlement regarding the service	<ul style="list-style-type: none"> <li>urn:mace:egi.eu:group:vo.example.eu:role=member:faai.egi.eu</li> <li>urn:mace:egi.eu:group:vo.example.eu:role=vm_operator:faai.egi.eu</li> <li>urn:mace:egi.eu:group:vo.example.eu:vo.example-sub.eu:role=member:faai.egi.eu</li> </ul>
Identity assurance profile	<ul style="list-style-type: none"> <li>https://refeds.org/assurance/IAP/low</li> <li>https://aai.egi.eu/LoAR/low</li> </ul>
eduPersonAssurance	

<https://snf-666522.vm.oceanos.grnet.gr/ssp/module.php/core/authenticate.php?as=egi-demo-sp>



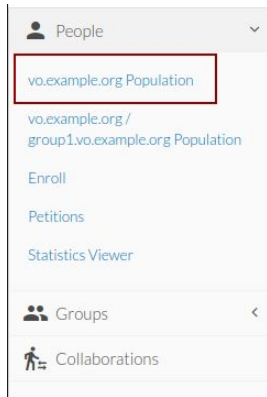
# Management of VO group members

## Removing member from VO group (1/2)

1) Expand the People drop down menu and click <VO-NAME> Population (for example, vo.example.org Population)



2) Find the user you want to add to the VO Group and click **Edit**.



EGI User Community People

Toggle All: Open Closed      Sort By: ▲ Name Status Created Modified

Filter

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	🔍

<https://docs.egi.eu/users/aai/check-in/vos/#removing-members>

# Management of VO group members

## Removing member from VO group (2/2)

3) From the VO members list, click **Edit** on the person that is going to be removed.



4) Under Role Attributes click **Delete** on the right of the COU entry of interest (for example, eossc-synergy.eu). On success the selected row will be removed.

Home > EGI User Community > My Population

EGI User Community People

Toggle All: Open Closed

Sort By: ▲ Name Status Created Modified

Filter																										
a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	⊞
▶	Valeria Ardizzone (valeria.ardizzone@egi.eu)	Active	<a href="#">Edit</a>																							
▶	Nikolaos Evangelou (nikosev@admin.gmet.gr)	Active	<a href="#">Edit</a>																							
▶	Ioannis Igoumenos (ioigoume@admin.gmet.gr)	Active	<a href="#">Edit</a>																							
▶	Nicolas Liampotis (nliam@gmet.gr)	Active	<a href="#">Edit</a>																							

Page 1 of 1. Viewing 1-4 of 4

Role Attributes

[Add](#)

COU	Title	Affiliation	Valid From	Valid Through	Status	Actions
eossc-synergy.eu		Member	2020-02-11 00:00:00	2021-02-10 00:00:00	Active	<a href="#">Edit</a> <a href="#">Relink</a> <a href="#">Delete</a>
service-integration.aai.egi.eu		Member	2020-02-10 00:00:00	2022-02-23 23:59:59	Active	<a href="#">Edit</a> <a href="#">Relink</a> <a href="#">Delete</a>

<https://docs.egi.eu/users/aai/check-in/vos/#removing-members>

### 1. Navigate to Co Person Role view

[Home](#) > [EGI User Community](#) > [My Population](#) > [Ioannis Igoumenos](#) > [Edit CO Person Role](#)

### 2. Choose Role from drop down list, if available, or add custom text if no list is present.

EGI User Community Title

A custom role can be assigned to a VO member during the Enrollment flow process if the user case requires it

# Role Management

## Removing role from VO member

From the VO members list (see Viewing VO members above):

1. Click Edit on the person that is going to be removed.

Home > EGI User Community > My Population

EGI User Community People

Toggle All:  Open  Closed

Sort By: ▲ Name Status Created Modified

Filter

a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	🔍
																								▶ Valeria Ardizzone (valeria.ardizzone@egi.eu)	Active	<a href="#">Edit</a>
																								▶ Nikolaos Evangelou (nikosev@admin.grnet.gr)	Active	<a href="#">Edit</a>
																								▶ Ioannis Igoumenos (ioigoume@admin.grnet.gr)	Active	<a href="#">Edit</a>
																								▶ Nicolas Liampotis (niliam@grnet.gr)	Active	<a href="#">Edit</a>

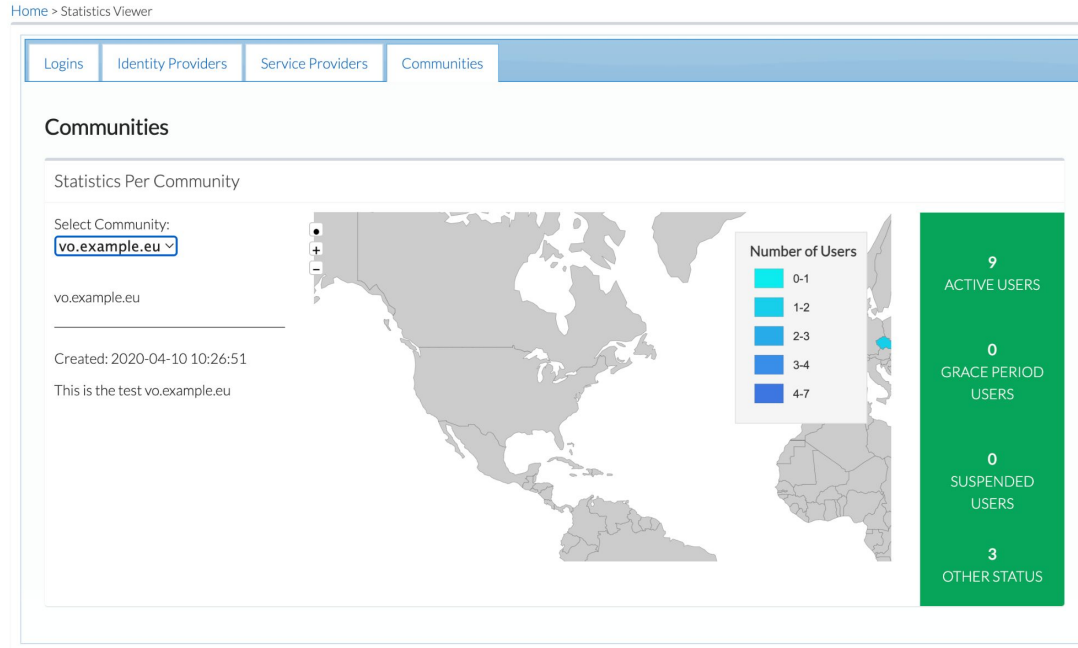
Page 1 of 1, Viewing 1-4 of 4

2. Under **Role Attributes** click **Delete** on the right of the COU entry of interest (for example, vo.example.com). On success the selected row will be removed. In this example we removed the **vo.geoss.eu** that we previously added.

Role Attributes [Add](#)

COU	Title	Affiliation	Valid From	Valid Through	Status	Actions
eosc-synergy.eu		Member	2020-02-11 00:00:00	2021-02-10 00:00:00	Active	<a href="#">Edit</a> <a href="#">Relink</a> <a href="#">Delete</a>
service-integration.aai.egi.eu		Member	2020-02-10 00:00:00	2022-02-23 23:59:59	Active	<a href="#">Edit</a> <a href="#">Relink</a> <a href="#">Delete</a>

## Accessible via **People** → **Statistics Viewer**



COMANAGE provides a REST API that allows VO managers to:

- Manage membership information only for the VOs they are authoritative for
- Retrieve VO group information only for the VOs they are authoritative for

Features:

- Members of the VO are identified via their EGI Check-in Community User Identifier (CUID)
- Membership can be limited to a specified period
- All [REFEDS](#) membership affiliations are supported
- Role titles are supported
- Different membership status values are supported, namely Active, Expired, Deleted, Suspended
- Check-in automatically changes the membership status from Active to Expired beyond the validity period

# VO Membership API

*Example: Adding VO member*

Requires specifying the following mandatory params:

- User's EGI Check-in identifier,
- Name of the VO (e.g. vo.example.eu),
- status (Active),
- valid from/through dates.

```
$ curl -vX POST $VO_API_BASE_URL.json \
  --user "example-client":"veryverysecret" \
  --data @add.json \
  --header "Content-Type: application/json"
```



```
{
  "RequestType": "CoPersonRoles",
  "Version": "1.0",
  "CoPersonRoles": [
    {
      "Version": "1.0",
      "Person": {
        "Type": "co",
        "Identifier": {
          "Type": "epuid",
          "Id": "01234567890123456789@egi.eu"
        }
      },
      "Cou": {
        "CoId": "2",
        "Name": "vo.example.org"
      },
      "Affiliation": "member",
      "Title": "Engineer",
      "Status": "Active",
      "ValidFrom": "2022-02-16 11:19:38",
      "ValidThrough": "2022-05-16 11:19:38"
    }
  ]
}
```

<https://docs.egi.eu/users/aai/check-in/vos/#vo-api>

# LDAP access to VO Membership information

Attribute	Description	Example
<code>objectClass</code>		<code>inetOrgPerson, eduPerson, voPerson, eduMember, ldapPublicKey</code>
<code>voPersonId</code>	Community User Identifier ( <code>voPersonID</code> )	<code>bef42b9ed8878c542555829cb21da3e25ad91a0f9cg54gsdcs35htf@egi.eu</code>
<code>uid</code>	user ID	<code>john.doe</code>
<code>cn</code>	Full name	<code>John Doe</code>
<code>displayName</code>	Full name	<code>John Doe</code>
<code>givenName</code>	First name	<code>John</code>
<code>sn</code>	Last name	<code>Doe</code>
<code>mail</code>	Email address	<code>john.doe@mail.com</code>
<code>edupersonUniqueID</code>	Community User Identifier (see also <code>voPersonId</code> )	<code>bef42b9ed8878c542555829cb21da3e25ad91a0f9cg54gsdcs35htf@egi.eu</code>
<code>eduPersonPrincipaName</code>	A scoped identifier for a person. The value is the same as the	<code>bef42b9ed8878c542555829cb21da3e25ad91a0f9cg54gsdcs35htf@egi.eu</code>
<code>eduPersonEntitlement</code>	URN that indicates a set of rights to specific resources	<code>urn:mace:egi.eu:group:vo.example.org:role=member#aai.egi.eu</code>
<code>sshPublicKey</code>	SSH public key	
<code>memberOf</code>	Group memberships	<code>CO:COU:vo.example.org:members</code>
<code>voPersonCertificateDN</code>	The Subject Distinguished Name of an X.509 certificate held by the person	<code>voPersonCertificateDN;scope-cert1: CN=John Doe A251,0=Example,C=US,DC=cilogon,DC=org</code>
<code>voPersonCertificateIssuerDN</code>	The Subject Distinguished Name of the X.509 certificate issuer	<code>voPersonCertificateIssuerDN;scope-cert1: CN=CILogon Basic CA 1, 0=CILogon, C=US, DC=cilogon, DC=org</code>



- [Usage guide](#)
- [Integration guide for service providers](#)
- [Integration guide for identity providers](#)

# EGI: Advanced Computing for Research



[www.egi.eu](http://www.egi.eu)

@EGI\_eInfra

Thank you  
for your attention.

*Questions?*



**This work by the EGI Foundation**  
is licensed under a Creative Commons  
Attribution 4.0 International License.



**The work of the EGI Foundation**  
is partly funded by the European Commission  
under H2020 Framework Programme

# Assurance: What is it?

## REFEDS Assurance Components & Profiles

Should identifiers be unique, personal and traceable?	Should identifiers be unique across the infrastructure?	How fresh do attributes need to be?	What kind of ID Proofing is required?	Is Multi-Factor Authentication required?
Unspecified	Unspecified	Unspecified	Unspecified	Unspecified
Yes	Yes	1 month	Low (self asserted)	Single factor authentication
			Medium (e.g. postal credential delivery)	Multifactor authentication
			High (e.g. face to face)	

**AARC Assam**  
**IGTF Dogwood**  
**RAF Cappuccino**  
**IGTF Birch**  
**RAF Espresso**

**New profiles!**

# Assurance: What is it?

## *EGI Check-in Profiles*

Based on the authentication method selected by the user, EGI Check-in Proxy assigns a Level of Assurance (LoA).

EGI Check-in currently distinguishes between three LoA levels. Each level is represented by a URI as follows:

- **Low:** Authentication through a social identity provider or other low identity assurance provider: `https://aai.egi.eu/LoA#Low`
- **Substantial:** Password/X.509 authentication at the user's home IdP: `https://aai.egi.eu/LoA#Substantial`
- **High:** Substantial + multi-factor authn (not supported yet): `https://aai.egi.eu/LoA#High`