

IDEM Entity Registry

Gestione Metadati e Adesione alla Federazione

Corso Shibboleth IdP - 22-23/01/2020

Marco Malavolti - marco.malavolti@garr.it

Agenda

- IDEM Entity Registry e l'ingresso in IDEM
- IDEM Entity Registry e le Entity Category
- IDEM Entity Registry e le Attribute Release Policy

IDEM Entity Registry e l'ingresso in IDEM

IDEM Entity Registry - Cos'è

IDEM Entity Registry è uno strumento web che colleziona e raccoglie i metadata delle entità, IdP e SP, che compongono la Federazione IDEM.

IDEM usa il registry per inserire le entità nelle sue federazioni:

1. IDEM Test Federation
2. IDEM Production Federation (IdP automaticamente aggiunti in eduGAIN, OPT-OUT)

Tale strumento serve ai Membri e ai Partner per gestire i propri metadata e creare filtri (attribute-filter) personalizzati verso risorse federate specifiche.

IDEM Entity Registry - Registrazione

- a) Inserimento dei metadati nel Registry in modalità «non autenticato»
- b) Approvazione in Federazione di TEST da parte del Servizio IDEM
- c) Log-in via IDEM con il nuovo IdP
- d) Consegna dei privilegi di scrittura da parte del Servizio IDEM all'utente
- e) Completamento del profilo dei metadati
- f) Verifiche di funzionamento in Federazione di TEST
- g) Approvazione nella Federazione IDEM

IDEM Entity Registry - Inserimento Metadata

IDEM Entity Registry

ITALIANO	ENGLISH
L>IDEM Entity Registry è l'applicazione, amministrata dalla Federazione IDEM, che si occupa della raccolta, della gestione e della visualizzazione dei suoi Metadati.	The IDEM Entity Registry is an application, provided by the IDEM Federation, that collects, manages and visualizes the federation's metadata.
Attraverso di essa gli utenti, amministratori e contatti tecnici, delle varie Organizzazioni potranno gestire le informazioni contenute nei propri metadati in modo facile e veloce attraverso una pratica interfaccia grafica.	With this application the users, administrators and technical contacts of different Organisations are able to manage the information contained in their metadata with a simple, fast and practical Graphics User Interface.
Per ricevere supporto rivolgersi a: IDEM Help	To receive support contact the: IDEM Help
Questo servizio rispetta la seguente Privacy Policy	This service follows this Privacy Policy
Fai LOG-IN per modificare le entità che hai già registrato.	To modify the metadata of your entities, please LOG-IN.
Per registrare una nuova entità utilizza i link sottostanti	To register new entities, use the links below.
<u>Inserisci un Nuovo Identity Provider nella IDEM Test Federation</u>	Insert a New Identity Provider into the IDEM Test Federation
Inserisci un Nuovo Service Provider nella IDEM Test Federation	Insert a New Service Provider into the IDEM Test Federation

Copiare e Incollare idp-metadata.xml



IDEM Entity Registry - Completamento Metadata

completare: Organization, Contacts, UI Information e SAML

Identity Provider registration form - advanced mode

General

Organization

Contacts

UI Information

UI Hints

SAML

Certificates

Federation ⓘ

IDEM Test Federation ▼

Your contact details

Given name

Nome

Surname

Cognome

Email

Indirizzo email|

Contact phone

Start over

Save draft

Register

IDEM Entity Registry - Completamento Metadata

General **Organization** Contacts UI Information UI Hints SAML Certificates

Name of organization

English (en) [Remove](#)

Italian (it) [Remove](#)

Abkhaz (ab)

Displayname of organization

English (en) [Remove](#)

Italian (it) [Remove](#)

Abkhaz (ab)

URL to information about organization

English (en) [Remove](#)

Italian (it) [Remove](#)

Abkhaz (ab)


[Start over](#) [Save draft](#) [Register](#)

IDEM Entity Registry - Best Practices

- Inserire i loghi nei seguenti formati
 - **Logo: 80 x 60 px** (o loro multipli)
 - **Favicon: 16 x 16 px** (o loro multipli)
- Inserire le **descrizioni** in doppia lingua: **Italiano/Inglese**
- Gli indirizzi **email** del supporto utenti (technical/support) devono essere **impersonali**.

IDEM Entity Registry e le Entity Category

IDEM Entity Registry - Entity Category

 Federations **Identity Providers** Service Providers Register Administration

List Of Identity Providers

DASHBOARD / IDENTITY PROVIDERS

Display 10 records per page

Showing 1 to 2 of 2 entries (filtered from 3,824 total records)

external/imported locally managed Column visibility

2 Search: garr-

3

Name of organization	URL to information about organization	Registration Date	status
PROD - IDP in the Cloud Project (GARR) https://garr-idp-prod.irccs.garr.it/idp/shibboleth	http://www.garr.it/b/eng	2015-07-08	
TEST - IDP in the Cloud Project (GARR) https://garr-idp-test.irccs.garr.it/idp/shibboleth	http://www.garr.it/b/eng		

Name of organization	URL to information about organization	Registration Date	status
----------------------	---------------------------------------	-------------------	--------

IDEM Entity Registry - Entity Category

The screenshot displays the IDEM Entity Registry interface. On the left, a sidebar contains a list of actions under the 'Actions' header, including 'Edit provider', 'Manage membership (joining)', 'Manage membership (leaving)', and 'Attributes'. A red arrow labeled '2' points to the 'Edit provider' option. The main content area shows the details for the 'Identity Provider: PROD - IDP in the Cloud Project (GARR)'. A red arrow labeled '1' points to the 'General' tab in the top navigation bar. Below the tabs, the 'Status' is 'Enabled', and the 'Last modification' is '2019-07-17 12:41:'. Other fields include 'EntityID' (https://garr-idp-prc), 'Name of organization' (it: Consortium GA, en: Consortium G), and 'Displayname of organization' (it: PROD - Proget, en: PROD - IDP ii).

Accedere alla modalità **"Edit provider"** per eseguire le **modifiche ai metadata** del proprio IdP

IDEM Entity Registry - Entity Category

PROD - IDP in the Cloud Project (GARR)

PROD - IDP IN THE CLOUD PROJECT (GARR) / EDIT

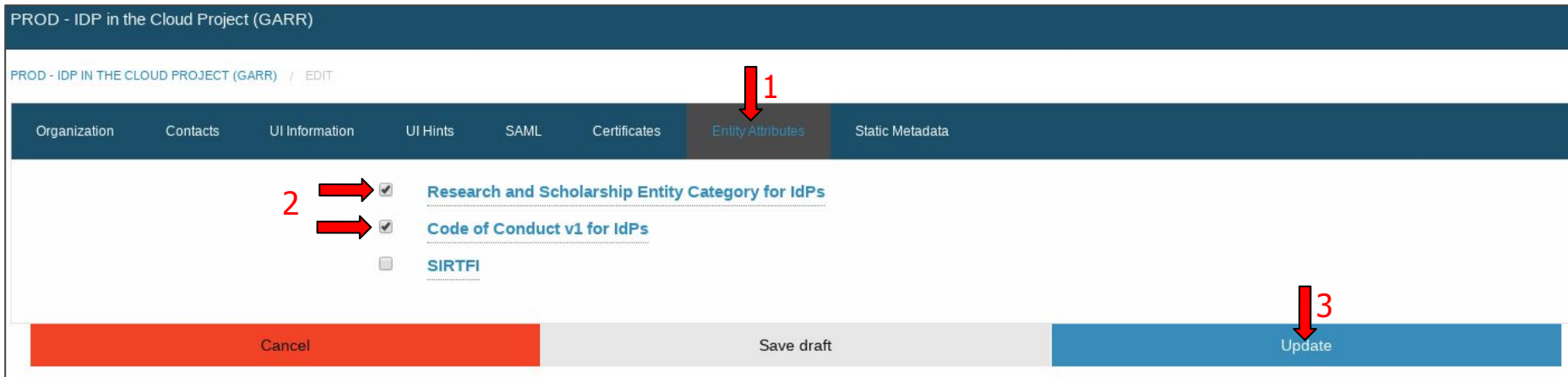
Organization Contacts UI Information UI Hints SAML Certificates **Entity Attributes** Static Metadata

2 → ☒ [Research and Scholarship Entity Category for IdPs](#)

→ ☒ [Code of Conduct v1 for IdPs](#)

☐ [SIRTFI](#)

Cancel Save draft **Update**



Dal tab **"Entity Attribute"** scegliere quali Entity Category chiedere di attivare e premere sul bottone **"Update"**

IDEM Entity Registry e le Attribute Release Policy

IDEM Entity Registry - ARP - Filtri personalizzati

The screenshot displays the IDEM Entity Registry ARP interface. On the left, a sidebar contains two main sections: 'Actions' and 'Attributes'. The 'Attributes' section is expanded, showing a list of options: 'SPs excluded from ARP', 'Attribute Policy', and 'Clear cache'. A red arrow labeled '2' points to the 'Attribute Policy' option. The main content area shows the configuration for 'Identity Provider: PROD - IDP IN THE CLOUD PROJECT (GARR)'. At the top, there are tabs for 'General', 'Membership', 'Metadata', 'Management', and 'Logs/Stats'. A red arrow labeled '1' points to the 'General' tab. Below the tabs, the 'Status' section is visible, followed by fields for 'Last modification', 'EntityID', 'Name of organization', 'Displayname of organization', 'URL to information about organization', 'Registration Authority', and 'Registration Date'.

IDEM Entity Registry - ARP - Filtri personalizzati

[Federations](#)[Identity Providers](#)[Service Providers](#)[Register](#)[Administration](#)[DASHBOARD](#) / [IDENTITY PROVIDERS](#) / [PROD - IDP IN THE CLOUD PROJECT \(GARR\)](#) / [ATTRIBUTE RELEASE POLICY](#)[Information](#)[Attributes/Default Policy](#)[Federations](#)[Entity Categories](#)[Service Providers](#)

INFORMATION GUIDE SOON!

- Default Attribute Release Policy - it does not include rules based on Entity Categories:

<https://registry.idem.garr.it/rr3/arp/format2/aHR0cHM6Ly9nYXJyLWlkcc1wcm9kLmlyY2NzLmdhcnluaXQvaWRwL3NoaWJib2xldGg~/arp.xml>

- Experimental Attribute Release Policy for ShibbolethIDP ver 2.x - it does include rules based on Entity Categories:

<https://registry.idem.garr.it/rr3/arp/format2exp/aHR0cHM6Ly9nYXJyLWlkcc1wcm9kLmlyY2NzLmdhcnluaXQvaWRwL3NoaWJib2xldGg~/arp.xml>

- Experimental Attribute Release Policy for ShibbolethIDP ver 3.x - it does include rules based on Entity Categories:

<https://registry.idem.garr.it/rr3/arp/format3exp/aHR0cHM6Ly9nYXJyLWlkcc1wcm9kLmlyY2NzLmdhcnluaXQvaWRwL3NoaWJib2xldGg~/arp.xml>

Fino a che le policy non saranno configurate,
queste Attribute Release Policy (alias Attribute Filters) saranno **vuote**.

IDEM Entity Registry - ARP - Filtri personalizzati

Ordine di priorità stabilite dal registro.
L'ultima sovrascrive la precedente:

1. Attributes/Default Policy
2. Federations
3. Entity Category
4. Service Providers

IDEM Entity Registry - ARP - Default Policy

Information Attributes/Default Policy Federations Entity Categories Service Providers

In modo predefinito vogliamo che **nessun** attributo sia rilasciato a **chiunque**.

1 Add attribute

Attribute name	Attribute support/default policy	Action
email	deny	
eduPersonAffiliation	deny	
3 eduPersonOrgUnitDN	deny	
eduPersonEntitlement	deny	
surname	deny	
givenName	deny	
uid	deny	
eduPersonPrincipalName	deny	
eduPersonTargetedID	deny	
eduPersonScopedAffiliation	deny	

2

Attribute eduPersonOrgUnitDN

Policy deny




Cancel Add

Nella Default Policy devono comparire gli **attributi supportati** dall'IdP.

IDEM Entity Registry - ARP - Federations Policy

Le policy sugli attributi valgono solo per gli SP delle federazioni di cui l'IdP è membro e sovrascrivono le Default

Information Attributes/Default Policy **Federations** Entity Categories Service Providers

Attribute name	Policy	Requirement	Action
Federation: IDEM Production Federation			
email	permit if required malavolti@garr.it (2020-01-14) : Permetto solo se necessario		
eduPersonEntitlement	permit if required malavolti@garr.it (2020-01-14) : Permetto solo se necessario		
surname	permit if required malavolti@garr.it (2020-01-14) : Permetto solo se necessario malavolti@garr.it (2020-01-14) : test test		
givenName	permit if required malavolti@garr.it (2020-01-14) : Permetto solo se neces		
eduPersonPrincipalName	permit if required		
eduPersonScopedAffiliation	permit if required		
Federation: idem2eduGAIN Federation			
eduPersonEntitlement	no policy malavolti@garr.it (2020-01-14) : test test		
eduPersonScopedAffiliation	no policy		
email	no policy		

IdP membro di

Attributi Supportati

Update policy based federarion

Attribute: email

Policy: permit if required

Comment: Permetto solo se necessario

Cancel Update

IDEM Entity Registry - ARP - Entity Category Policy

InformationAttributes/Default PolicyFederationsEntity CategoriesService Providers

Add new policy

Attribute name	Policy	Action
EntityCategory: http://macedir.org/entity-category http://refeds.org/category/research-and-scholarship		
email	permit if required or desired malavolti@garr.it (2020-01-14) : Permetto il rilascio anche se n	
givenName	permit if required or desired malavolti@garr.it (2020-01-14) : Permetto anche se non richies	
eduPersonPrincipalName	permit if required or desired malavolti@garr.it (2020-01-14) : Permetto il rilascio anche se n	

Add policy based on Entity Category

AttributegivenName

Entity Categoryhttp://refeds.org/category/research-and-scholarship

Policypermit if required or desired

CommentPermetto anche se non richiesto

Cancel

Update

1

2

3

Le policy definiscono il comportamento dell'IdP nel rilasciare gli attributi agli SP che seguono e rispettano le Entity Category indicate.

IDEM Entity Registry - ARP - Service Providers

InformationAttributes/Default PolicyFederationsEntity CategoriesService Providers

Add new policy

1

Attribute name	Policy
https://sdatauth.sciencedirect.com/	
eduPersonEntitlement	<div>3</div> <div>permit if required</div> <div>permitted values: urn:mace:dir:entitlement:common-lib-terms,</div>
eduPersonTargetedID	no policy

2

Add policy based on Service Provider

Attribute

eduPersonEntitlement

Service Provider

Elsevier (https://sdatauth.sciencedirect.com/)

Policy

permit if required

Enable policy

☒

based on values

custom policy

permitted values

Values (use comma for multi value)

urn:mace:dir:entitlement:common-lib-terms

Comment

Permetti il rilascio dell'attributo ePE valorizzato a "urn:mace:dir:entitlement:common-lib-terms"

Cancel

Update

Le policy definiscono le regole di rilascio degli attributi che l'IdP seguirà verso gli SP stabiliti.

(L'esempio mostra come sia possibile rilasciare un attributo valorizzato in un certo modo ad uno specifico SP)

IDEM Entity Registry - ARP - Download

[Information](#) [Attributes/Default Policy](#) [Federations](#) [Entity Categories](#) [Service Providers](#)

INFORMATION GUIDE SOON!

- Default Attribute Release Policy - it does not include rules based on Entity Categories:
<https://registry.idem.garr.it/rr3/arp/format2/aHR0cHM6Ly9nYXJyLWlkC1wcm9kLmlyY2NzLmdhcnluaXQvaWRwL3NoaWJib2xldGg~/arp.xml>
- Experimental Attribute Release Policy for ShibbolethIDP ver 2.x - it does include rules based on Entity Categories:
<https://registry.idem.garr.it/rr3/arp/format2exp/aHR0cHM6Ly9nYXJyLWlkC1wcm9kLmlyY2NzLmdhcnluaXQvaWRwL3NoaWJib2xldGg~/arp.xml>
- Experimental Attribute Release Policy for ShibbolethIDP ver 3.x - it does include rules based on Entity Categories:
<https://registry.idem.garr.it/rr3/arp/format3exp/aHR0cHM6Ly9nYXJyLWlkC1wcm9kLmlyY2NzLmdhcnluaXQvaWRwL3NoaWJib2xldGg~/arp.xml>

Una volta configurate le Policy sarà possibile recuperare, dalla scheda **"Information"**, i file di configurazione (attribute-filter) per il proprio IdP in due modi:

1. Prelevando il file dalle URL indicate
2. Cliccando su  e copiando il codice sorgente della pagina

Tale recupero può avvenire anche dinamicamente dal proprio IdP attraverso tali URL e gestire così il rilascio degli attributi completamente da IDEM Resource Registry senza toccare la configurazione dell'IdP.

IDEM Entity Registry - ARP - Download

```
<?xml version="1.0"?>
<afp:AttributeFilterPolicyGroup xmlns:afp="urn:mace:shibboleth:2.0:afp" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
urn:mace:shibboleth:2.0:afp:mf:basic classpath:/schema/shibboleth-2.0-afp-mf-basic.xsd urn:mace:shibboleth:2.0:
<!--
```

```
=====

Attribute Release Policy for Consortium GARR (https://garr-idp-prod.irccs.garr.it/idp/shibboleth)

generated on Tue Jan 14 16:26:14 CET 2020

=====
```

```
-->
<!--
XploreUAT Digital Library Explorer test SP provided by IEEE
-->
<afp:AttributeFilterPolicy id="https://xploreuat.ieee.org/shibboleth-sp">
  <afp:PolicyRequirementRule xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="basic:AttributeR
  <afp:AttributeRule attributeID="eduPersonScopedAffiliation">
    <afp:PermitValueRule xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="basic:ANY"/>
  </afp:AttributeRule>
  <afp:AttributeRule attributeID="eduPersonTargetedID">
    <afp:PermitValueRule xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xsi:type="basic:ANY"/>
  </afp:AttributeRule>
</afp:AttributeFilterPolicy>
<!--
RefWorks test SP erogato da RefWorks-COS, a division of ProQuest LLC
-->
```

Domande?

marco.malavolti@garr.it
giuseppe.demarco@unical.it
maurizio.festi@unitn.it