



THE ITALIAN
EDUCATION
& RESEARCH
NETWORK

IDEM Entity Registry

Come gestire gli incidenti di sicurezza e l'accesso alle risorse in ambito federato

IDEM DAYS 2021

Marco Malavolti - marco.malavolti@garr.it

Davide Vaghetti - davide.vaghetti@garr.it

Agenda

- IDEM Entity Registry e la Federazione IDEM
- IDEM Entity Registry e le Entity Attribute/Category
- IDEM Attribute Filters (per Shibboleth)
- IDEM Entity Registry e le Attribute Release Policy

IDEM Entity Registry e la Federazione in IDEM

IDEM Entity Registry e la Federazione IDEM

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

Il Servizio IDEM usa il registry per:

1. registrare le nuove entità
2. aggiungere le Entity Category supportate dalle entità
3. gestire i filtri statici per il rilascio degli attributi

Tale strumento è utile ai Membri e ai Partner per:

1. gestire i propri metadata con semplicità e in autonomia
2. creare filtri personalizzati per le risorse IDEM ed eduGAIN

Entity Attribute/Category

Entity Attribute/Category

Le Entity Attribute/Category supportate da IDEM per IdP e SP sono riportate alla pagina:

<https://wiki.idem.garr.it/wiki/EntityAttribute-Category>

Il Servizio IDEM esegue un controllo accurato dei requisiti necessari che le entità richiedenti devono rispettare per richiederne l'abilitazione (generalmente prima di entrare nella Federazione IDEM).

Richiesta abilitazione COCO Entity Category

GÉANT Data Protection Code of Conduct (COCO):

1. Verificare il possesso dei requisiti indicati dalla pagina ufficiale della specifica:

<https://wiki.refeds.org/display/CODE/Data+Protection+Code+of+Conduct+Home>

2. Completare la relativa sezione su IDEM Entity Registry:

(Edit Provider -> Entity Attribute -> spunta su "Code of Conduct v1 for IdPs" o "Code of Conduct v1 for SP")

3. Attendere l'approvazione del servizio IDEM:

il supporto a COCO apparirà nei metadati della vostra entità a partire dall'ora successiva l'approvazione del servizio IDEM-help

Richiesta abilitazione R&S Entity Category

REFEDS Research and Scholarship (R&S):

1. Verificare il possesso dei requisiti indicati dalla pagina ufficiale della specifica:

<https://refeds.org/category/research-and-scholarship>

2. Completare la relativa sezione su IDEM Entity Registry:

(Edit Provider -> Entity Attribute -> spunta su "Research and Scholarship Entity Category for IdPs" o "Research and Scholarship Entity Category for SP")

3. Attendere l'approvazione del servizio IDEM:

il supporto a R&S apparirà nei metadati della vostra entità a partire dall'ora successiva l'approvazione del servizio IDEM-help

Richiesta abilitazione SIRTFI Entity Attribute

Security Incident Response Trust Framework for Federated Identity (SIRTFI):

1. Effettuare una "*autovalutazione*" assicurandosi di aver risposto positivamente a tutte le affermazioni contenute nel documento:

<https://refeds.org/wp-content/uploads/2016/01/Sirtfi-1.0.pdf>

(OS1-OS6, IR1-IR6, TR1-TR2, PR1-PR2)

2. Esclusivamente per i membri della Federazione IDEM
il Servizio IDEM *consiglia* di uniformare il Security Contact a:
 - a. Given name = GARR-CERT
 - b. Email = cert@garr.it

In questo modo tutti gli scambi di informazioni relativi agli incidenti verranno esclusivamente condotti con questo contatto.

Richiesta abilitazione SIRTFI Entity Attribute

3. Completare la relativa sezione su IDEM Entity Registry:

- a. (Contacts -> Add Contact -> [Type=Security (SIRTFI), Given name=NAME, email=EMAIL])
- b. (Edit Provider -> Entity Attribute -> spunta su SIRTFI)

4. Attendere l'approvazione del servizio IDEM:

il supporto a SIRTFI apparirà nei metadati della vostra entità a partire dall'ora successiva l'approvazione del servizio IDEM-help

IDEM Entity Registry e Entity Attribute/Category

GÉANT Data Protection Code of Conduct & REFEDS Research and Scholarship

IDEM Entity Registry - Identity Providers

IDEM Entity Registry - <https://registry.idem.garr.it>

1 → 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)

2 → external/imported locally managed Column visibility

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

Accedere alla risorsa IDEM Entity Registry e spostarsi nello spazio riservato al proprio IdP attraverso la scheda **"Identity Providers"**

IDEM Entity Registry - Service Providers

IDEM Entity Registry - <https://registry.idem.garr.it>

Federations Identity Providers **Service Providers** Register Administration EN

List Of Service Providers

DASHBOARD / SERVICE PROVIDERS

Display records per page

external/imported locally managed Column visibility

Showing 1 to 1 of 1 entries (filtered from 3,868 total records)

2 Search:

Name of the Service	URL to information about organization	Registration Date	status
3 SP Demo provided by GARR	http://www.garr.it/en	2019-01-03	

Accedere alla risorsa IDEM Entity Registry e spostarsi nello spazio riservato al proprio SP attraverso la scheda **"Service Providers"**

IDEM Entity Registry - Edit Provider

The screenshot shows the 'Edit provider' interface for the 'PROD - IDP in the Cloud Project (GARR)' identity provider. The left sidebar contains a menu with 'Actions' and 'Attributes'. The 'Actions' menu is expanded, showing 'Edit provider' (highlighted with a red arrow labeled '2'), 'Manage membership (joining)', and 'Manage membership (leaving)'. The 'Attributes' menu shows 'SPs excluded from ARP', 'Attribute Policy', and 'Clear cache'. The main content area has a header 'Identity Provider: PROD - IDP in the Cloud Project (GARR)' and a GARR logo. Below the header, there's a tabbed interface with 'General', 'Membership', 'Metadata', 'Management', and 'Logs/Stats'. The 'General' tab is selected (highlighted with a red arrow labeled '1'). It displays the provider's status as 'Enabled', last modification time as '2019-07-17 12:41:', EntityID as 'https://garr-idp-prc', Name of organization as 'it: Consortium GA en: Consortium G', and Displayname of organization as 'it: PROD - Proget en: PROD - IDP ii'.

Attivare la modalità **"Edit provider"** per eseguire le **modifiche ai metadata** del proprio IdP/SP

IDEM Entity Registry - COCO / R&S

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

Se fosse un Service Provider (SP):

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

→ ☒ [Code of Conduct v1 for IdPs](#)

☐ [SIRTFI](#)

☒ [Code of Conduct v1 for SP](#)

☒ [Research and Scholarship Entity Category for SP](#)

Cancel Save draft Update

1

3

Dalla scheda **"Entity Attributes"** scegliere per quali fare la richiesta di attivazione e premere sul bottone **"Update"**

SIRTFI

**(Security Incident
Response Trust
Framework for
Federated Identity)**

IDEM Entity Registry - Identity Providers

IDEM Entity Registry - <https://registry.idem.garr.it>

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

Search: garr-

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

Accedere alla risorsa IDEM Entity Registry e spostarsi nello spazio riservato al proprio IdP attraverso la scheda **"Identity Providers"**

IDEM Entity Registry - Service Providers

IDEM Entity Registry - <https://registry.idem.garr.it>

Federations Identity Providers **Service Providers** Register Administration EN

List Of Service Providers

DASHBOARD / SERVICE PROVIDERS

Display records per page

external/imported locally managed Column visibility

Showing 1 to 1 of 1 entries (filtered from 3,868 total records)

2 Search:

Name of the Service	URL to information about organization	Registration Date	status
3 SP Demo provided by GARR	http://www.garr.it/en	2019-01-03	

Accedere alla risorsa IDEM Entity Registry e spostarsi nello spazio riservato al proprio SP attraverso la scheda **"Service Providers"**

IDEM Entity Registry - SIRTFI (IDP/SP)

The screenshot displays the IDEM Entity Registry interface. On the left, a sidebar contains two main sections: 'Actions' and 'Attributes'. The 'Actions' section includes 'Edit provider' (highlighted with a red arrow and the number 2), 'Manage membership (joining)', and 'Manage membership (leaving)'. The 'Attributes' section includes 'SPs excluded from ARP', 'Attribute Policy', and 'Clear cache'. The main content area shows the 'Identity Provider: PROD - IDP in the Cloud Project (GARR)' configuration. A red arrow and the number 1 point to the 'General' tab, which is selected. The 'General' tab displays the following information:

Field	Value
Status	Enabled Manage
Last modification	2019-07-17 12:41:
EntityID	https://garr-idp-prc
Name of organization	it: Consortium GA en: Consortium G
Displayname of organization	it: PROD - Proget en: PROD - IDP ii

Attivare la modalità **"Edit provider"** per eseguire le **modifiche ai metadata** del proprio IdP/SP

IDEM Entity Registry - SIRTFI

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

Contact

1 ↑

Type

Given name

Surname

Email

2 ←

Aggiungere un **nuovo contatto** con il bottone blu **"Add contact"**

IDEM Entity Registry - SIRTFI

Contact

Type

Security (Sirty) ← 1

Given name

GARR-CERT ← 2

Surname

Email

cert@garr.it ← 3

Remove contact

Add contact

Cancel

Save draft

Update

4

Completare le informazioni del **nuovo contatto** e confermare premendo sul bottone blu **"Update"**

IDEM Entity Registry - SIRTFI

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

☐ [Research and Scholarship Entity Category for IdPs](#)

☐ [Code of Conduct v1 for IdPs](#)

☒ [SIRTFI](#) ← 1

Cancel Save draft Update

2 ↑

Aprire la sezione **"Entity Attributes"**,
scegliere **"SIRTFI"** e
confermare la richiesta premendo sul bottone blu **"Update"**

Domande?

IDEM Attribute Filters

IDEM Attribute Filters

Il Servizio IDEM GARR AAI offre ai membri della sua comunità diversi filtri utilizzabili per il rilascio degli attributi:

<https://wiki.idem.garr.it/wiki/RilascioAttributi>

ARP	Tipo	Attributi Richiesti	Attributi Opzionali	Attributi SP IDEM di Test	Attributi SP Custom	Attributi Entity Category
<u>static</u>	statico	X	X			
<u>fed</u>	dinamico	X		X		
<u>custom</u>	statico				X	
<u>ec</u>	dinamico					X
<u>full</u>	dinamico	X		X	X	X

IDEM Attribute Filters

- **static** (statico): IDP3 | IDP4
contiene le regole di rilascio degli attributi Obbligatori e Opzionali alle risorse di IDEM che li dichiarano nei metadata
- **fed** (dinamico): IDP3 | IDP4
contiene le regole per il rilascio di:
 - tutti gli attributi possibili agli SP di Test di IDEM
 - tutti gli attributi necessari a IDEM Entity Registry
 - tutti gli attributi necessari all'accesso alle risorse federate in IDEM
 - eduPersonTargetedID (se non è supportato il *persistent* NameID o se non è indicato tra i RequestedAttribute dei metadata del SP)
 - eduPersonScopedAffiliation a tutte le risorse federate in IDEM

IDEM Attribute Filters

- **custom** (statico): IDP3 | IDP4
contiene le regole di rilascio degli attributi per le risorse che seguono regole particolari sui valori rilasciati o che non dichiarano i RequestedAttribute nei metadata
- **ec** (dinamico): IDP3 | IDP4
contiene le regole di rilascio degli attributi per gli SP che implementano le EntityAttribute-Category supportate in IDEM.
- **full** (dinamico): IDP3 | IDP4
custom + **fed** + **ec**

IDEM Entity Registry e le Attribute Release Policy

IDEM Entity Registry - ARP - Filtri personalizzati

IDEM Entity Registry - <https://registry.idem.garr.it>

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

Search: garr-

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		

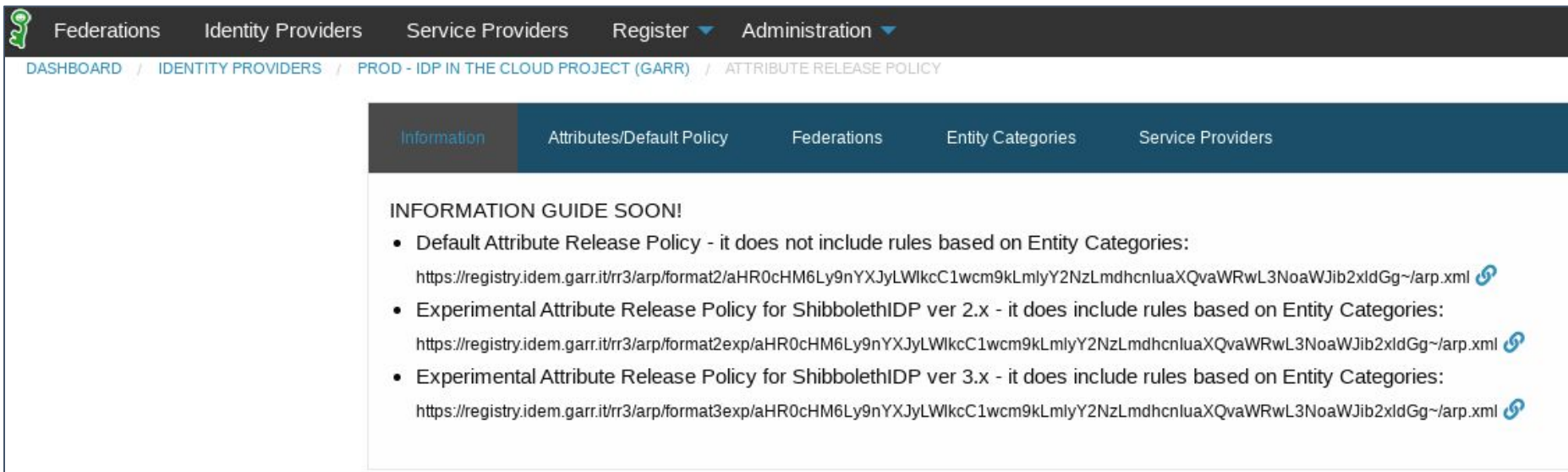
Name of organization URL to information about organization Registration Date status

Accedere alla risorsa IDEM Entity Registry e spostarsi nello spazio riservato al proprio IdP attraverso la scheda **"Identity Providers"**

IDEM Entity Registry - ARP - Filtri personalizzati

The screenshot displays the IDEM Entity Registry ARP interface. On the left, a sidebar contains a menu with 'Actions' and 'Attributes' sections. The 'Attributes' section is expanded, showing 'SPs excluded from ARP', 'Attribute Policy', and 'Clear cache'. A red arrow labeled '2' points to 'Attribute Policy'. The main content area shows the 'Identity Provider: PROD - IDP in the Cloud Project (GARR)' configuration. A red arrow labeled '1' points to the 'General' tab in the configuration panel. The 'General' tab is active, displaying fields for 'Status', '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



The screenshot shows the IDEM Entity Registry web interface. The top navigation bar includes links for Federations, Identity Providers, Service Providers, Register, and Administration. Below this, a breadcrumb trail indicates the current path: DASHBOARD / IDENTITY PROVIDERS / PROD - IDP IN THE CLOUD PROJECT (GARR) / ATTRIBUTE RELEASE POLICY. The main content area has a tabbed interface with 'Information' selected. The 'Information' tab displays a message: 'INFORMATION GUIDE SOON!' followed by a list of three items:

- 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 da IDEM Entity Registry,
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	

Attribute eduPersonOrgUnitDN

Policy 2 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			
<u>email</u>	permit if required malavolti@garr.it (2020-01-14) : Permetto solo se necessario		
<u>eduPersonEntitlement</u>	permit if required malavolti@garr.it (2020-01-14) : Permetto solo se necessario		
<u>surname</u>	permit if required malavolti@garr.it (2020-01-14) : Permetto solo se necessario malavolti@garr.it (2020-01-14) : test test		
<u>givenName</u>	permit if required malavolti@garr.it (2020-01-14) : Permetto solo se neces		
<u>eduPersonPrincipalName</u>	permit if required		
<u>eduPersonScopedAffiliation</u>	permit if required		
Federation: idem2eduGAIN Federation			
<u>eduPersonEntitlement</u>	no policy malavolti@garr.it (2020-01-14) : test test		
<u>eduPersonScopedAffiliation</u>	no policy		
<u>email</u>	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

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

1

Add new policy

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/aHR0cHM6Ly9nYXJyLWlkZC1wcm9kLmlyY2NzLmdhcmluaXQvaWRwL3NoaWJib2xldGg~/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/aHR0cHM6Ly9nYXJyLWlkZC1wcm9kLmlyY2NzLmdhcmluaXQvaWRwL3NoaWJib2xldGg~/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/aHR0cHM6Ly9nYXJyLWlkZC1wcm9kLmlyY2NzLmdhcmluaXQvaWRwL3NoaWJib2xldGg~/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

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

davide.vaghetti@garr.it