

SEE Identity Federation Training

Jagger Federation management tool :
How to use Jagger Interface

Jagger (ResourceRegistry3) is a web application developed by HEAnet to manage the Edugate multiparty SAML federation. Also Jagger can be used to manage federation, web-of-trust for a single entity or as GUI for the Shibboleth SAML Identity Provider, offering proper Attribute Filter functionality for it. Jagger also offer possibility to enrich IdPs metadata by adding missing attributes requested by target SPs.

Jagger requirements, description, and other useful information can be found at

<https://jagger.heanet.ie>

GitHub with latest changes is located at

<https://github.com/Edugate/Jagger>

Identity Federation has two main parts:

- *legal*
- *technical*

Legal part consists from:

- **agreements, policies, declarations** and other **formal stuff**.

Technical part have to deal with hardware, software and data exchange. Federation data flow consists from metadata transferred between: entities within federation or federation and eduGAIN. To sign and publish metadata or get downstream metadata from eduGAIN, *Jagger Resource Registry* is the simplest tool to be used.

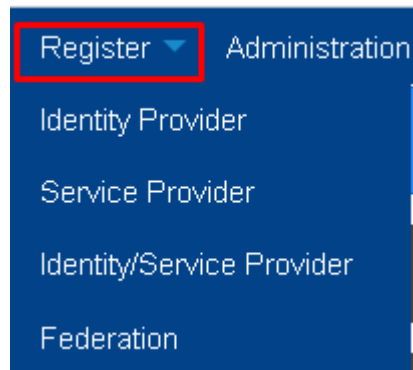
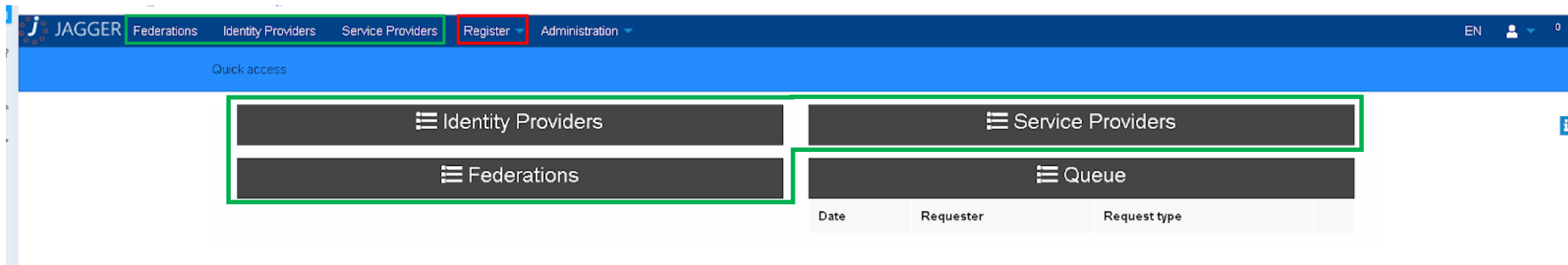
Federation management using Jagger

Few simple steps should be performed, to manage any identity federation using Jagger RR:

1. Populate federation data
2. Populate entities data
 - Add SP entity
 - Add IdP entity
3. Configure metadata sign process

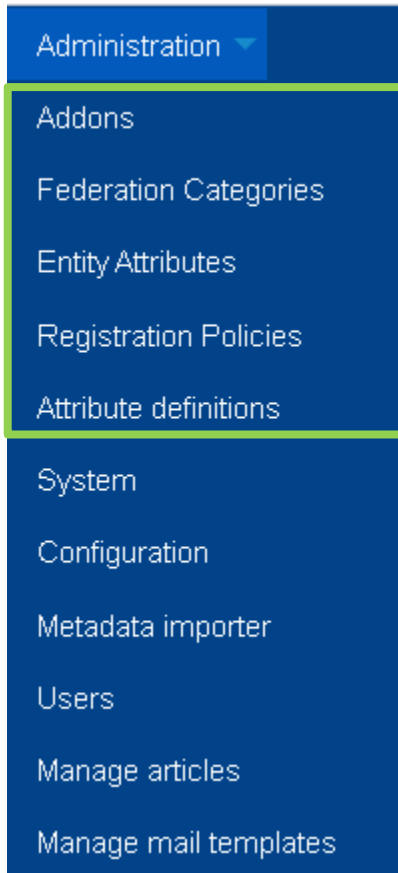
Default page

Jagger home page contains quick access buttons to registered federations, entities and actions queue.



Register button - from top navigation menu - will be used to start new Federation, Service Provider or Identity provider registration process

Administration menu



Administration menu offer a set of tools useful for federation or entity management.

Addons – SAML data decoder, useful decrypt encoded AuthnRequest / AuthnResponse: SAML Messages

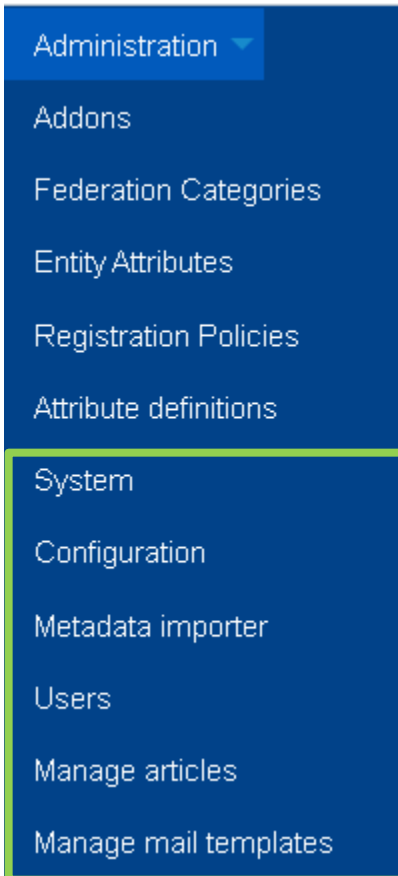
Federation Categories – create internal categories, and sort Federations into them

Entity Attributes – register attributes, linked to entities metadata

Registration Policies – manage Registration Policies, which can be used by entities or federations

Attribute definitions – manage list of SAML attributes exchangeable between IDP and SP

Administration menu



System – contain tools for system tests, and mass email sender (ex:to announce maintenance works)

Configuration – manage miscellaneous UI settings, like cookie consent for every page, custom text within interface header/footer, breadcrumbs, etc.

Metadata Importer - tool used to register entities by importing metadata.

Users – UI users manager

Manage articles – mini CMS used to create and manage home page

Manage mail templates – create and manage mail templates, used to request approval from federation manager.

Administration menu. Registration Policies

- Administration
- Addons
- Federation Categories
- Entity Attributes
- Registration Policies**
- Attribute definitions
- System
- Configuration
- Metadata importer
- Users
- Manage articles
- Manage mail templates

Registration policies can be used by multiple entities.

[Add Registration Policy](#)

Display Name	Language	URL of a document	Description	Status	Action
AESM Registration policy	en	http://idp.vle.ase.md/index.php/Policy	Place were registration policy of this organization are placed.	Enabled 1	
Federation Policy Agreement	en	http://federations.renam.md	Policy	Enabled 2	
http://federations.renam.md	ru	http://federations.renam.md	http://federations.renam.md	Disabled 1	
http://federations.renam.md	ro	http://federations.renam.md	http://federations.renam.md	Disabled 0	

List entities connected to RegistrationPolicy ✕

- [GIDP-RENAM \(https://gidp.federations.renam.md\)](https://gidp.federations.renam.md)
- [Federation Management Board \(https://manage.federations.renam.md\)](https://manage.federations.renam.md)

Administration menu

- Administration
- Addons
- Federation Categories
- Entity Attributes
- Registration Policies
- Attribute definitions
- System
- Configuration**
- Metadata importer
- Users
- Manage articles
- Manage mail templates

System preferences

Name	Description	Values	Status	Action
Category: general				
show cookie consent	option allows to display consent cookie on the top of page	Company uses cookies to your browsing experience and to create a secure and effective website for our customers. By using this site you agree that we may temporary store and access cookies on your devices, unless you have disabled your cookies	Disabled	✎
Category: page				
Text on the bootom page	Footer - Allow to add additional text on the bottom page	Powered by Jagger	Enabled	✎
Header title prefix	Text added as prefix into header title on a page	Jagger ::	Disabled	✎
show breadcrumbs	option allows to display breadcrumbs	This field is not used for settings	Disabled	✎
show title/subtitle on page	option allows to show/hide title on the page	This field is not used for settings	Enabled	✎
Category: authn				
Allow ordinary user set 2F	If enabled then any user can enable/disable 2F authentication otherwise only Administrator can do it	This field is not used for settings	Disabled	✎
Category: mail				
mail signature	mail signature added to every notication		Enabled	✎

Administration menu - Metadata importer

- Administration ▾
- Addons
- Federation Categories
- Entity Attributes
- Registration Policies
- Attribute definitions
- System
- Configuration
- Metadata importer**
- Users
- Manage articles
- Manage mail templates

Import Metadata

Metadata location URL

Type of entities

Federation

Metadata location URL

Don't validate the server's certificate

Options

Import entities as external or internal

Overwrite locally managed entities?

New entities enabled by default

Populate all information

Should static metadata be enabled by default

Metadata validation (optional)

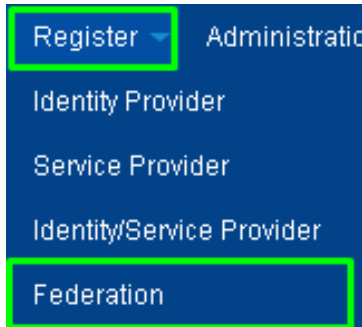
Validate metadata with certificate

URL of metadata signing certificate

Metadata signing certificate in X509 format
overwrites URL of cert

Register new Federation

Register new Federation into the Resource Registry is quite easy.



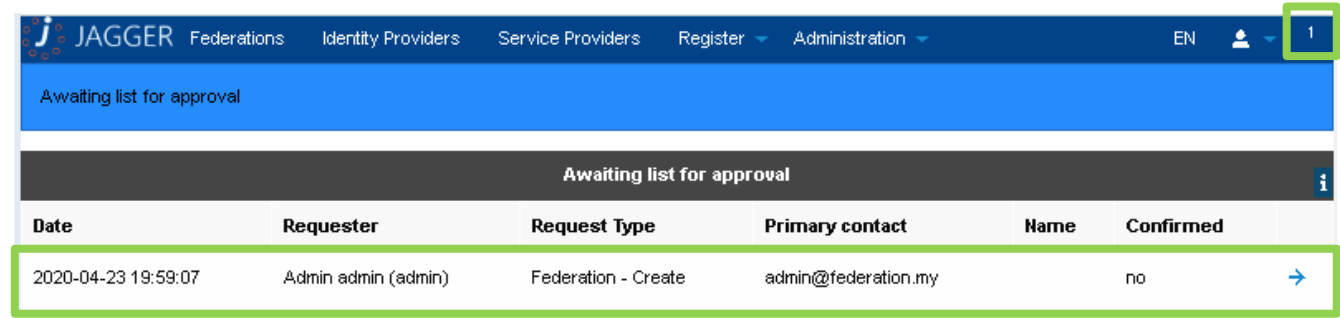
But it should be done using values defined in registration documents applied to eduGAIN

Federation registration form

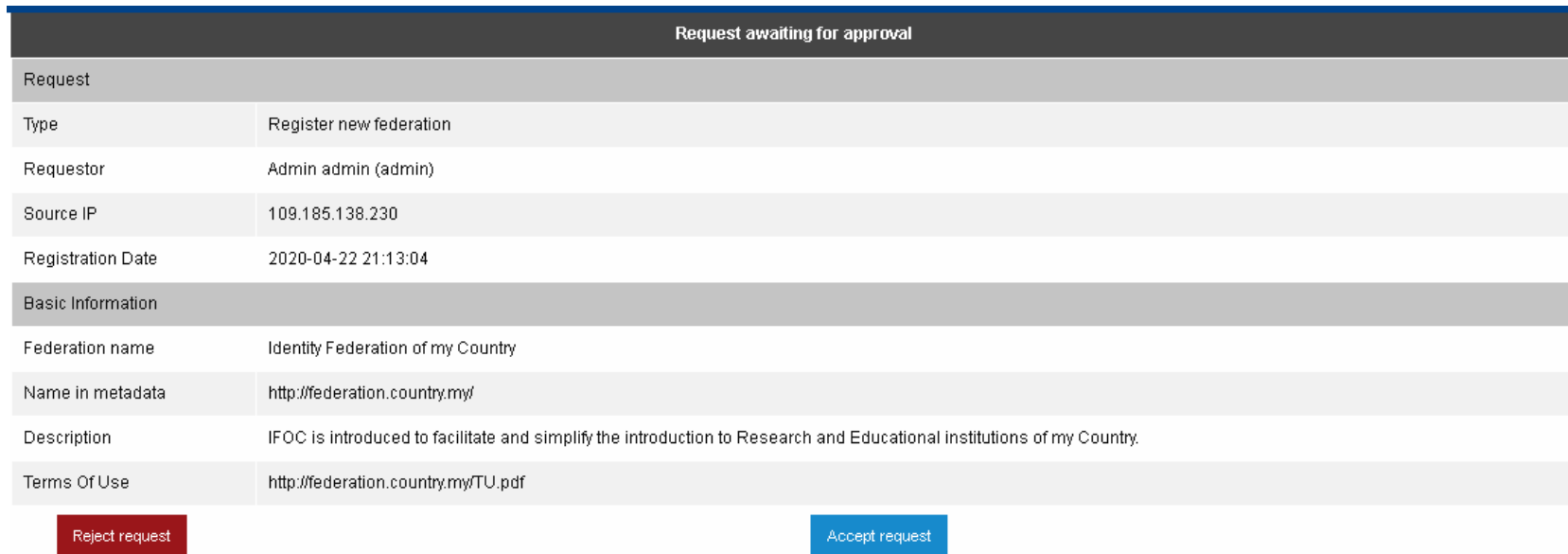
Internal/system name	<input type="text" value="IFOC"/>
Federation name	<input type="text" value="Identity Federation of my Country"/>
Name in metadata	<input type="text" value="http://federation.country.my/"/>
Access	Details visible to other users <input checked="" type="checkbox"/>
Description	<input type="text" value="IFOC is introduced to facilitate and simplify the introduction to Research and Educational institutions of my Country."/>
Terms Of Use	<input type="text" value="http://federation.country.my/TU.pdf"/>

Register new Federation

Newly registered federation will not appear in federations list until it is not validated by Jagger admin (even if requester is admin).



Date	Requester	Request Type	Primary contact	Name	Confirmed
2020-04-23 19:59:07	Admin admin (admin)	Federation - Create	admin@federation.my		no



Request awaiting for approval	
Request	
Type	Register new federation
Requestor	Admin admin (admin)
Source IP	109.185.138.230
Registration Date	2020-04-22 21:13:04
Basic Information	
Federation name	Identity Federation of my Country
Name in metadata	http://federation.country.my/
Description	IFOC is introduced to facilitate and simplify the introduction to Research and Educational institutions of my Country.
Terms Of Use	http://federation.country.my/TU.pdf

[Reject request](#) [Accept request](#)

Manage Federation

Approved federation will be populated with information provided and, if visible, is available for entities registration into it. In order to modify or delete federation, it should be deactivated first.

The screenshot shows the 'General' tab of the Manage Federation interface. It contains the following information:

Federation name	Identity Federation of my Country
Name in metadata	http://federation.country.my/
Internal/system name	ILOC1
EntitiesDescriptor ID	prefix-20200423120736 generated dynamically
Publisher	
Publisher (in export metadata)	
Description	ILOC is introduced to facilitate and simplify the introduction to Research and Educational institutions of my Country.
Terms Of Use	http://federation.country.my/TU.pdf
Download contacts list in txt format	Contact list of IdP members Contact list of SP members Contact list of all federation members
Timeline	Diagram

Request to deactivate federation

The screenshot shows the 'Management' tab of the Manage Federation interface. It contains the following information:

Access management →

[Deactivate Federation](#)

Active and inactive federation

Name	Name in metadata	Status
My1 stTF	manage.all.for.me	not public inactive
Identity Federation of my Country	http://federation.country.my/	not public active

Request to activate or delete federation

The screenshot shows the 'Management' tab of the Manage Federation interface. It contains the following information:

Access management →

[Activate Federation](#) [Apply to remove Federation](#)

Manage Federation

Active federation offer 4 metadata sources, also, 2 types of metadata are available: signed and unsigned. Unsigned metadata is aggregated immediately, accordingly to selected type, so it is fresh at every button press. Signed metadata is aggregated after *sign* button press, or using pre-configured periodic system job. Signed metadata will display last aggregated during signing job.

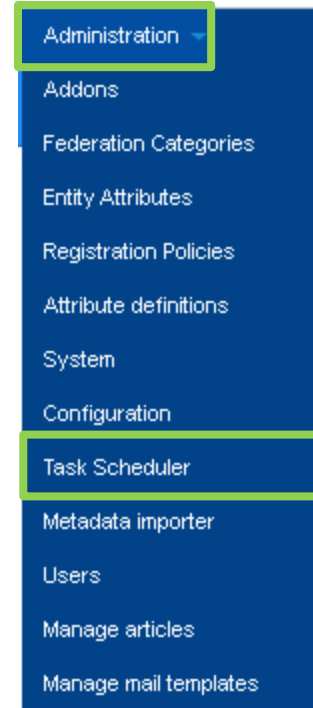
Federation details for: Identity Federation of my Country

General	Membership	Metadata	Attributes	Validators	Management
Federation metadata public link (unsigned)			http://81.180.84.235/rr3/metadata/federation/IFOC1/metadata.xml →		
Federation metadata public link (unsigned) only Identity Providers			http://81.180.84.235/rr3/metadata/federation/IFOC1/IDP/metadata.xml →		
Federation metadata public link (unsigned) only Service Providers			http://81.180.84.235/rr3/metadata/federation/IFOC1/SP/metadata.xml →		
Federation metadata public link (signed) SHA-1			http://81.180.84.235/rr3/signedmetadata/federation/IFOC1/metadata.xml →		
Sign metadata			sign		

Manage Federation. Task Scheduler tool

Preconfigured periodic system job can be runned by Jagger integrated *Task Scheduler*. It will become available in *Administration* menu if enabled in configuration files. Time format to run task is similar to *Linux crontab*.

Job accept input parameters, paired as *key*<>*value*. Exists two levels of parameters: which define *action* and which define required *parameter*.



Task scheduler interface. New job.

Minute	Hour	Day of month	Month	Day of week
<input type="text" value="1"/>	<input type="text" value="8"/>	<input type="text" value="*"/>	<input type="text" value="*"/>	<input type="text" value="*"/>
Task enabled?	<input type="checkbox"/>			
Description	<input type="text"/>			
Task template?	<input type="checkbox"/>			
Worker function name	<input type="text"/>			
Worker fn params	<input type="button" value="Add params"/>			

Manage Federation. Adding job to sign metadata

Job type *metadatasigner* – metadata sing.

type <> *federation* > *sysname* <> *short name of federation* (value)

provider > *entityid* <> *id of local managed entity* (value)

bulk > *name* <> *providers* – sign all entities metadata one by one
federations – sign all federations metadata
all – sign all entities and federations metadata

Shown configuration will apply *metadatasigner* job at 7:55, 11:55, 15:55, 19:55 every day. Job will sign all entities and federations metadata using provided certificate.


Minute	Hour	Day of month	Month	Day of week
<input type="text" value="55"/>	<input type="text" value="7,11,15,19"/>	<input type="text" value="*"/>	<input type="text" value="*"/>	<input type="text" value="*"/>
Task enabled?	<input checked="" type="checkbox"/>			
Description	<input type="text" value="bulk metadata sign"/>			
Task template?	<input checked="" type="checkbox"/>			
Worker function name	<input type="text" value="metadatasigner"/>			
Worker fn params	arg name	arg value	arg name	arg value
	<input type="text" value="type"/>	<input type="text" value="bulk"/>	<input type="text" value="name"/>	<input type="text" value="all"/>


Manage entities

New entities can be added by automatic population of registry from their instance metadata or manually introducing all needed information. There are two ways to add entities into Jagger using their metadata, by using *Register* menu or metadata importer tool from *Administration* menu.

Import metadata form called from Register menu

Identity Provider registration form

Metadata (optional) 


Register  Administration


Identity Provider


Service Provider

Identity/Service Provider

Federation



Next 

- Administration 
- Addons
- Federation Categories
- Entity Attributes
- Registration Policies
- Attribute definitions
- System
- Configuration
- Metadata importer
- Users
- Manage articles
- Manage mail templates

Add entity using metadata. XML insert

Adding entity by importing its metadata in *Registry* menu, can be done by inserting SAML 2.0 XML formatted metadata into form. Inserted metadata is parsed and shown within registry internal data categories.

```
<?xml version="1.0"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi" xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui"
xmlns:ds="http://www.w3.org/2000/09/xmldsig#" entityID="https://federation.my">
  <md:Extensions>
    <mdrpi:RegistrationInfo xmlns:mdrpi="urn:oasis:names:tc:SAML:metadata:rpi"
registrationAuthority="https://federation.my">
      <mdrpi:RegistrationPolicy xml:lang="ro">https://federation.my</mdrpi:RegistrationPolicy>
      <mdrpi:RegistrationPolicy xml:lang="en">https://federation.my</mdrpi:RegistrationPolicy>
      <mdrpi:RegistrationPolicy xml:lang="ru">https://federation.my</mdrpi:RegistrationPolicy>
    </mdrpi:RegistrationInfo>
  </md:Extensions>
  <md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:Extensions>
      <mdui:UIInfo xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui">
        <mdui:DisplayName xml:lang="en">IPOCIDP</mdui:DisplayName>
        <mdui:Description xml:lang="en">IPOCIDO - identity provider used by IPOC</mdui:Description>
        <mdui:InformationURL xml:lang="en">https://federation.my</mdui:InformationURL>
        <mdui:InformationURL xml:lang="ru">https://federation.my</mdui:InformationURL>
        <mdui:Logo width="285" height="121">https://myawesome.logo/my.jpg</mdui:Logo>
      </mdui:UIInfo>
    </md:Extensions>
  </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

Next

General Organization Contacts UI Information UI Hints SAML Certificates

Federation ⓘ No public federations found

Your contact details

Username	admin
Given name	Admin
Surname	admin
Email	admin@federation.my

Start over Save draft Register

Add entity using metadata. URL import

Metadata location URL

Type of entities: Identity Providers

Federation: Identity Federation of my Country

Metadata location URL: https://federation.mysaml2/idp/metadata.php

Don't validate the server's certificate:

Options

Import entities as external or internal: Local entities

Overwrite locally managed entities?: no

New entities enabled by default: yes

Populate all information: yes

Should static metadata be enabled by default: yes

Adding entity by importing its metadata in *Administration* menu, can be done by defining import options and metadata location.

Options offer possibility to define the way how added entity will be inserted into registry.

Internal/external entity – entity can/cannot be managed from Jagger UI

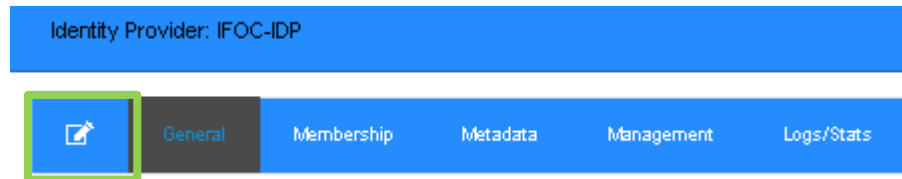
Static metadata – upstream entity metadata will not be affected by metadata tweaks from Jagger metadata explorer

Manage Federation entities

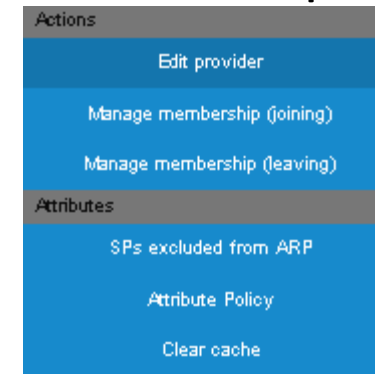
Metadata of internal entities can be edited by selecting entity from list.

Name of organization	URL to information about organization	Registration Date	status
IFOC-IDP https://idp.federation.my	http://federation.my		

Use *actions* button



Select action to perform



Edit provider – switch information tab to edit mode, so entity values can be edited

Manage membership – manage entity membership interface.

SPs excluded from ARP – manage list of SPs excluded from Attribute Release Policies

Attribute Policy – manage Attribute Release Policies

Clear cache – clears cached data thus updating displayed information

Manage Federation entities. Membership

Membership menu offer possibility to manage entity affiliation, state, sign and view metadata. Using *suspend* buttons, entity can be temporary disabled and kept in federation. *Administratively suspended* action is available only for Registry Administrator. If entity is suspended using *Administratively suspended*, *temporary suspend* state are not took into account. By pressing *Show members* button, the list of entities, available in same federation(s), will be shown*.

The screenshot shows a web interface with a blue header bar containing navigation tabs: General, Membership (highlighted with a green box), Metadata, Management, and Logs/Stats. In the top right corner, there are 'Leave' and 'Join' buttons. Below the header is a 'Metadata' section with the following fields:

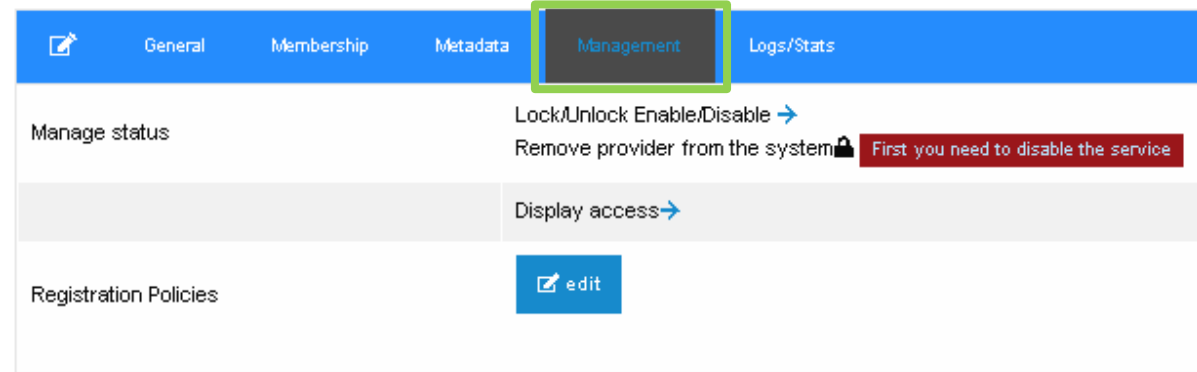
- Service metadata url: metadata url: →
- Circle of trust metadata URL: metadata url: →
- Circle of trust metadata URL (signed): metadata url: →
- Sign metadata: sign
- Member of: My1stTF Public metadata url: →

Below the 'Member of' field, there are two buttons: 'temporary suspend' and 'administratively suspend'. At the bottom of the interface, there is a 'Show members' button.

*if current entity is SP then IdP entities will be shown

Manage Federation entities. State management

Management menu offer possibility to adjust entity management type, state, validity period, etc.



The screenshot shows a navigation bar with tabs: General, Membership, Metadata, Management (highlighted with a green box), and Logs/Stats. Below the tabs, there are several options: 'Manage status' with a link 'Lock/Unlock Enable/Disable →', 'Remove provider from the system' with a lock icon and a red warning box 'First you need to disable the service', 'Display access →', and 'Registration Policies' with an 'edit' button.

Lock/Unlock Enable/Disable

Status management

Lock entity	<input type="text" value="Unlocked"/>	
Entity active	<input type="text" value="Enabled"/>	
Visibility on public list(s)	<input type="text" value="Visible on public lists"/>	
Entity as locally managed/external	<input type="text" value="Managed locally"/>	
Valid From	<input type="text" value="YY-MM-DD"/>	<input type="text" value="HH:mm"/>
Valid Until	<input type="text" value="YY-MM-DD"/>	<input type="text" value="HH:mm"/>

Display access

Access management

Username	read	write	manage
admin (Admin admin) <input type="button" value="You"/> <input type="button" value="Administrator"/>	has access	has access	has access

Invitation

Email	<input type="text"/>
Email confirm	<input type="text"/>
Access level	<input type="text" value="Select"/> <input type="text" value="Select"/> <input type="text" value="Edit resource"/> <input type="text" value="Manage resource"/>

Manage Federation entities. Removal

Entity removal actions

The screenshot shows the 'Management' tab selected in a navigation bar. Below the navigation bar, there are three main sections: 'Manage status', 'Registration Policies', and 'Display access'. The 'Remove provider from the system' link is highlighted with a green box. The 'edit' button is also visible.

Any entity or federation can be removed from registry. Remove option become accessible when entity or federation is disabled.

Federation removal actions

The screenshot shows the 'Management' tab selected in a navigation bar. Below the navigation bar, there is a red banner indicating 'Federation is inactive'. Below this, there is an 'Access management' section with two buttons: 'Activate Federation' and 'Apply to remove Federation'.

The dialog box has a title bar 'Remove provider from the system'. Below the title bar, there is a text input field containing 'https://awesomesp.federation.my'. Below the input field, there are two buttons: 'Cancel' and 'Remove provider from the system'.

Thank you

Any questions?

www.geant.org

