INDIGO IAM - status and evolution plans

Roberta Miccoli, Enrico Vianello
INFN-CNAF

INDIGO IAM User's Workshop
CERN, 10-11 October, 2022

INDIGO Identity and Access Management Service

First developed in the context of the **H2020 INDIGO DataCloud** project

Selected by the WLCG management board to be the core of the future, token-based WLCG AAI

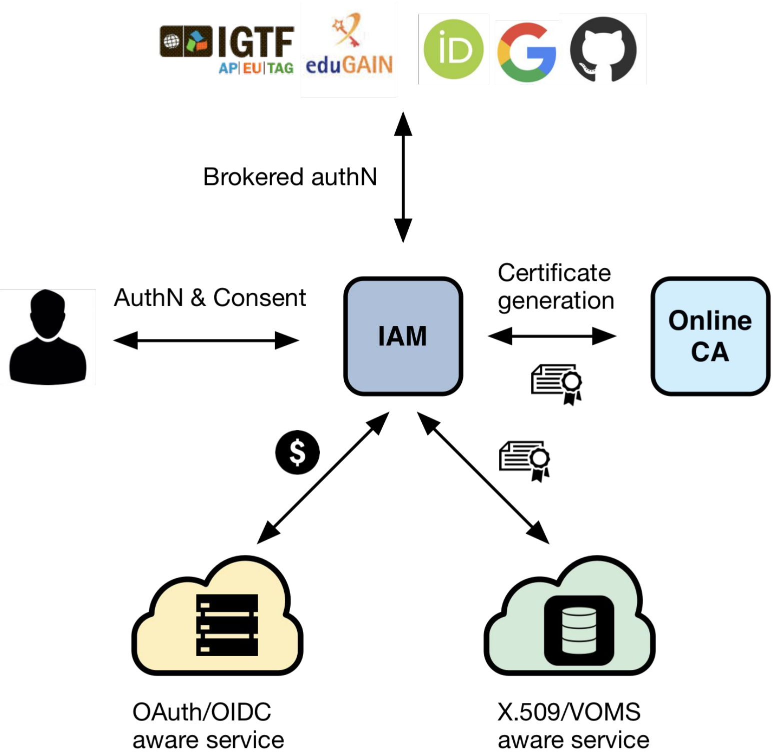
Commitment by INFN for the foreseeable future, with current support from:

ESCAPE

EOSC Pillar

EGI-ACE

EOSC Future



IGTF AP|EU|TAG

eduGAIN

Brokered authN

AuthN & Consent

IAM

Certificate generation

Online CA

OAuth/OIDC aware service

X.509/VOMS aware service

INDIGO IAM: the development team

IAM is mainly developed by the Software Development (SD) group at INFN-CNAF, with some much appreciated contributions from other parties

We are currently six people working on middleware (mainly INDIGO IAM, StoRM, VOMS, Argus):

- Francesco Giacomini (Lead)
- Enrico Vianello
- Federica Agostini
- Marcelo Soares
- Roberta Miccoli
- Tommaso Diotalevi

INDIGO IAM v1.8.0

Latest release: IAM v1.8.0 (1/4)

Released on: **2022-09-09**

Highlights:

- Spring Boot upgrade
- Refactored client management & registration
- JWT-based client authentication
- More support for AARC guidelines
- New consent page

other minor **improvements** & **bug fixes**

Latest release: IAM v1.8.0 (2/4)

Significant **changes** when upgrading from IAM v1.7.2

- About configuration:
  - **`IAM_USE_FORWARDED_HEADERS`** has been deprecated.
    - Use **`IAM_FORWARD_HEADERS_STRATEGY`** instead with value *native*, if you're deploying behind a reverse proxy, or *none* otherwise (default).
  - **`IAM_CLIENT_USE_FORWARDED_HEADERS`** has been deprecated.
    - Use **`IAM_CLIENT_FORWARD_HEADERS_STRATEGY`** instead with value *native*, if you're deploying behind a reverse proxy, or *none* otherwise (default).
  - **`IAM_CLIENT_SCOPES`** value is now parsed as a list of space-delimited scopes

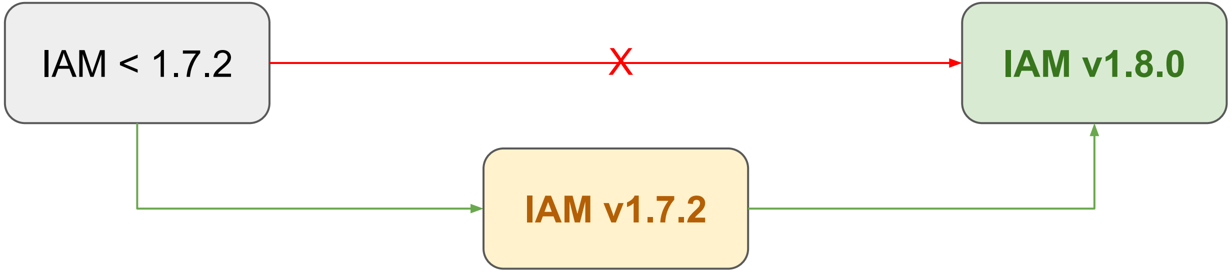
Latest release: IAM v1.8.0 (3/4)

Significant **changes** when upgrading from IAM v1.7.2

- About monitoring:
  - The **`/health`** endpoint and its children have been moved to **`/actuator/health`** base path.
    IAM v1.8.0 will still support and forward requests to the old endpoints.
    This forward will be removed on IAM v1.8.1.
- About compliance with draft OAuth 2.1:
  - Client redirect URIs and pre-registered URIs are compared using exact string matching (read more here).
- Others:
  - Token exchange not allowed if the actor and the subject are the same client and **`offline_access`** is among the requested scopes (more info here)

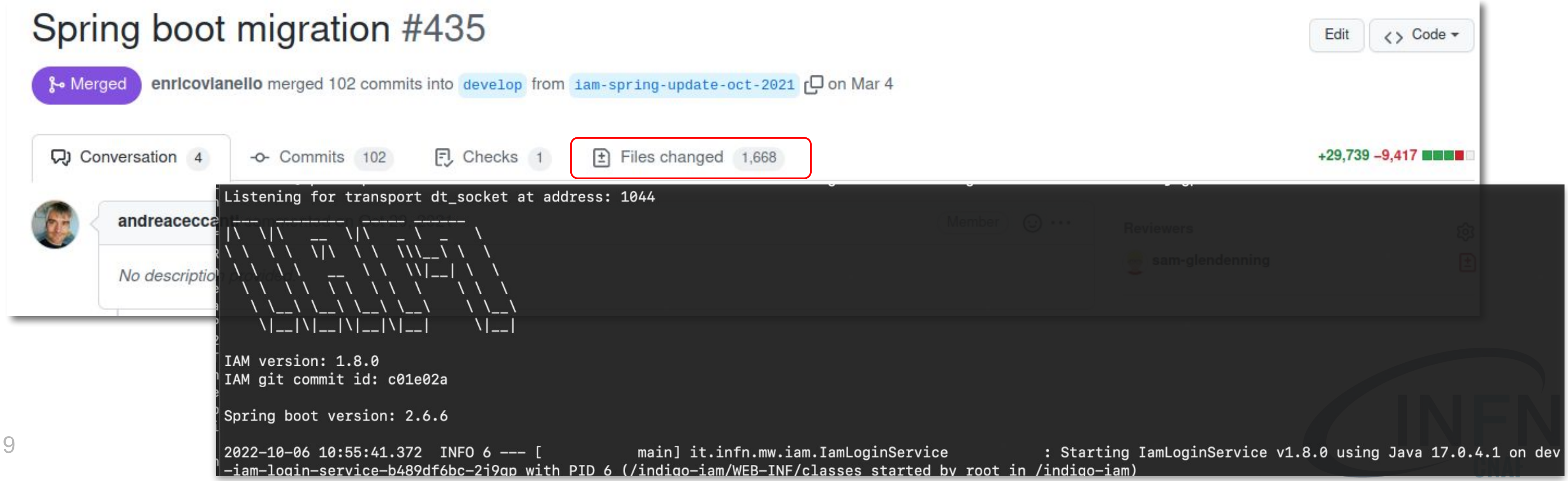
Latest release: IAM v1.8.0 (4/4)

- If you’re upgrading from IAM versions < 1.7.2 you **MUST** upgrade to v1.7.2 before.
  - Otherwise it won't work due to a problem described here and mainly related to the spring boot upgrade.



Spring Boot upgrade

INDIGO IAM is a Spring Boot application.
IAM v1.7.2 Spring Boot version (1.3.8) reached EOL so it’s been upgraded to **2.6.6**.
The upgrade allowed also to move to **Java 17**.



Spring boot migration #435

enricovianello merged 102 commits into develop from iam-spring-update-oct-2021 on Mar 4

andreacecca

No descriptio

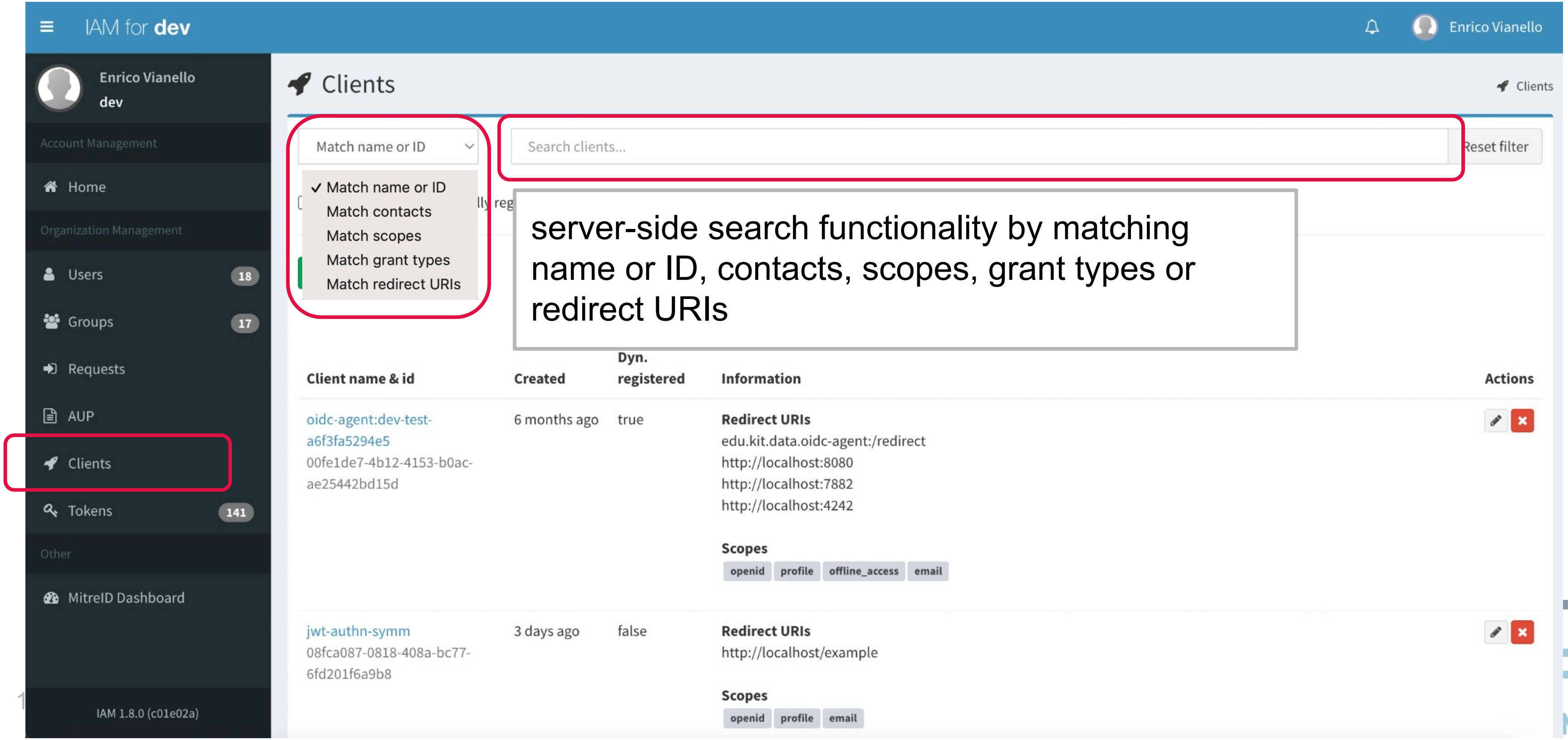
```
Listening for transport dt_socket at address: 1044
 ___  _______   _____  ______
|\  \|\   __  \|\   _ \  _   \
\ \  \ \  \|\  \ \  \\\__\ \  \
 \ \  \ \   __  \ \  \\|__| \  \
  \ \  \ \  \ \  \ \  \    \ \  \
   \ \__\ \__\ \__\ \__\    \ \__\
    \|__|\|__|\|__|\|__|     \|__|

IAM version: 1.8.0
IAM git commit id: c01e02a

Spring boot version: 2.6.6

2022-10-06 10:55:41.372  INFO 6 --- [           main] it.infn.mw.iam.IamLoginService           : Starting IamLoginService v1.8.0 using Java 17.0.4.1 on dev
-iam-login-service-b489df6bc-2j9qp with PID 6 (/indigo-iam/WEB-INF/classes started by root in /indigo-iam)
```

Refactored client management & registration (1/6)

The new IAM client management & registration API solves several scalability and usability limits of old MITREid Connect API:

- No pagination on client management APIs causes issues on the management dashboard with large number of clients
  - The new API implements **pagination**
- No client search API
  - The new API implements a **server-side search functionality**

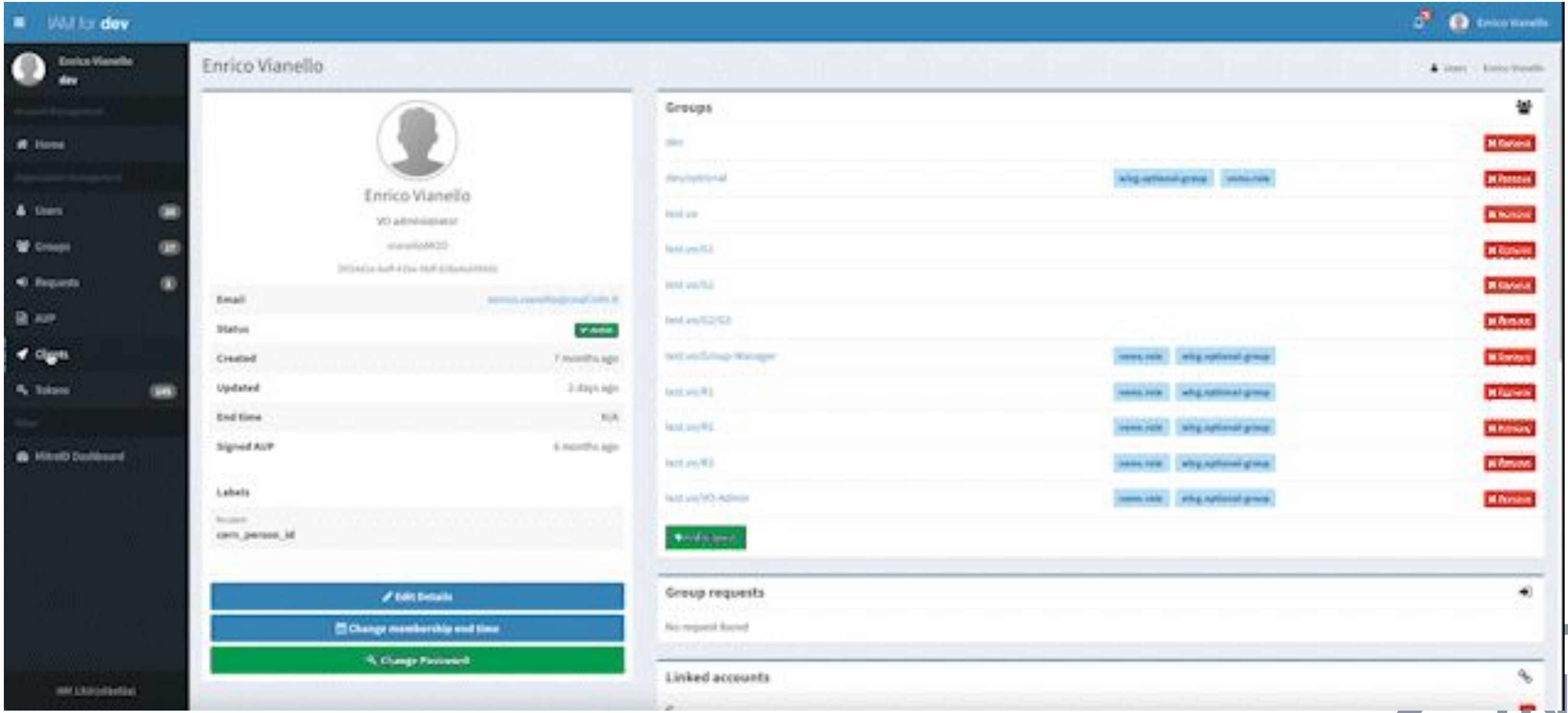
Refactored client management & registration (2/6)



server-side search functionality by matching name or ID, contacts, scopes, grant types or redirect URIs

Client name & id	Created	Dyn. registered	Information	Actions
oidc-agent:dev-test-a6f3fa5294e5 00fe1de7-4b12-4153-b0ac-ae25442bd15d	6 months ago	true	**Redirect URIs** edu.kit.data.oidc-agent:/redirect http://localhost:8080 http://localhost:7882 http://localhost:4242 **Scopes** openid profile offline_access email	✎ ✖
jwt-authn-symm 08fca087-0818-408a-bc77-6fd201f6a9b8	3 days ago	false	**Redirect URIs** http://localhost/example **Scopes** openid profile email	✎ ✖

Refactored client management & registration (3/6)



IAM for **dev**

Enrico Vianello

dev

- Home
- Users
- Groups 27
- Requests
- AUP
- Clients
- Tokens
- MitreID Dashboard

Enrico Vianello

Enrico Vianello

VO administrator

Email	
Status	✓ Active
Created	7 months ago
Updated	2 days ago
End time	N/A
Signed AUP	6 months ago

Labels

cern_person_id

Edit Details

Change membership end time

Change Password

Groups

dev		Remove
dev/optional	wlcg.optional-group voms.role	Remove
test.vo		Remove
test.vo/G1		Remove
test.vo/G2		Remove
test.vo/G2/G3		Remove
test.vo/Group-Manager	voms.role wlcg.optional-group	Remove
test.vo/R1	voms.role wlcg.optional-group	Remove
test.vo/R1	voms.role wlcg.optional-group	Remove
test.vo/R3	voms.role wlcg.optional-group	Remove
test.vo/VO-Admin	voms.role wlcg.optional-group	Remove

Add to group

Group requests

No request found

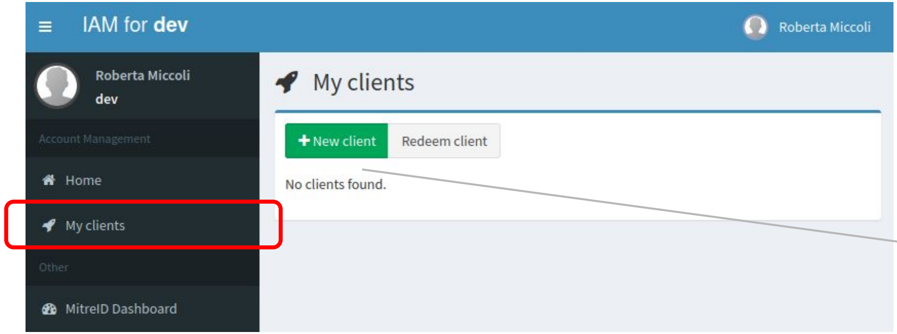
Linked accounts

Refactored client management & registration (4/6)

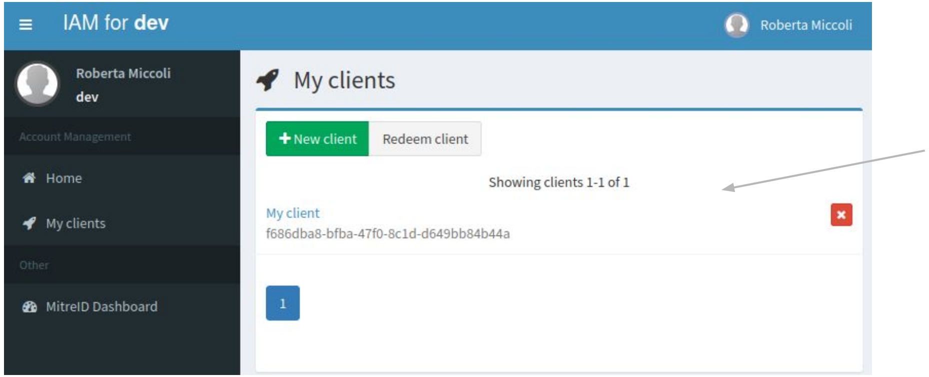
The new IAM client management & registration API solves several scalability and usability limits of old MitreID Connect API:

- Client management always requires to use registration access tokens, making it hard for users to have a clear view of their registered clients
  - users can **see and manage from IAM dashboard all the clients linked to their account**
  - old registration access token can be used to **redeem** and link a client to user’s personal account

Refactored client management & registration (5/6)

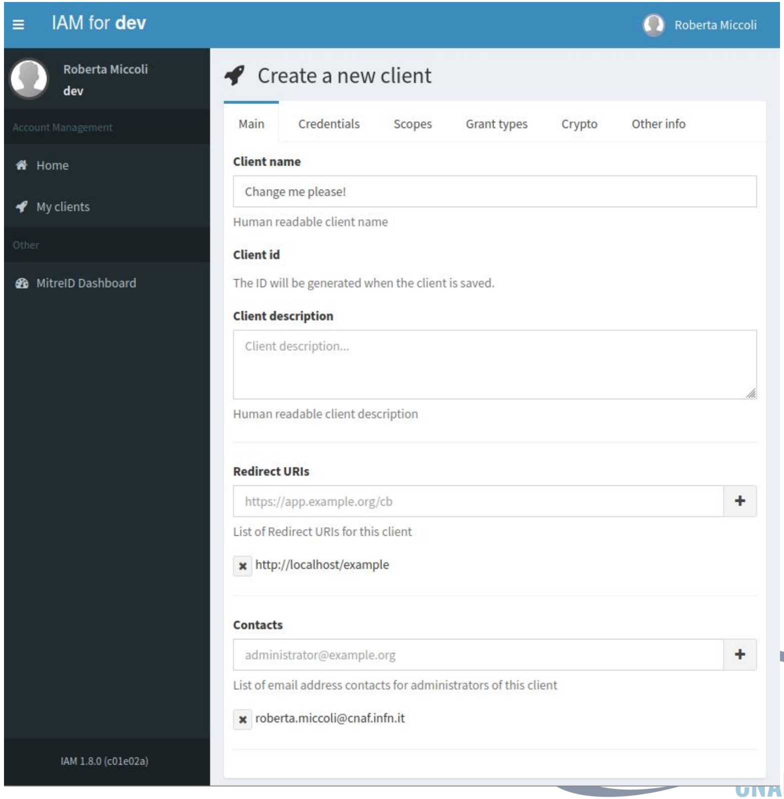


No clients found.



Showing clients 1-1 of 1

My client
f686dba8-bfba-47f0-8c1d-d649bb84b44a



Client name

Change me please!

Human readable client name

Client id

The ID will be generated when the client is saved.

Client description

Client description...

Human readable client description

Redirect URIs

https://app.example.org/cb +

List of Redirect URIs for this client

✖ http://localhost/example

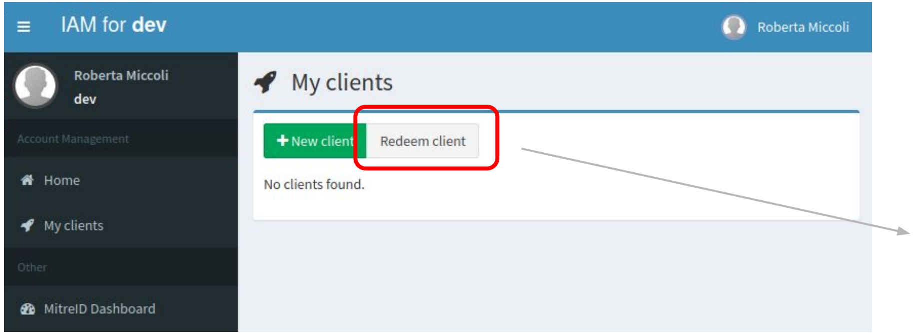
Contacts

administrator@example.org +

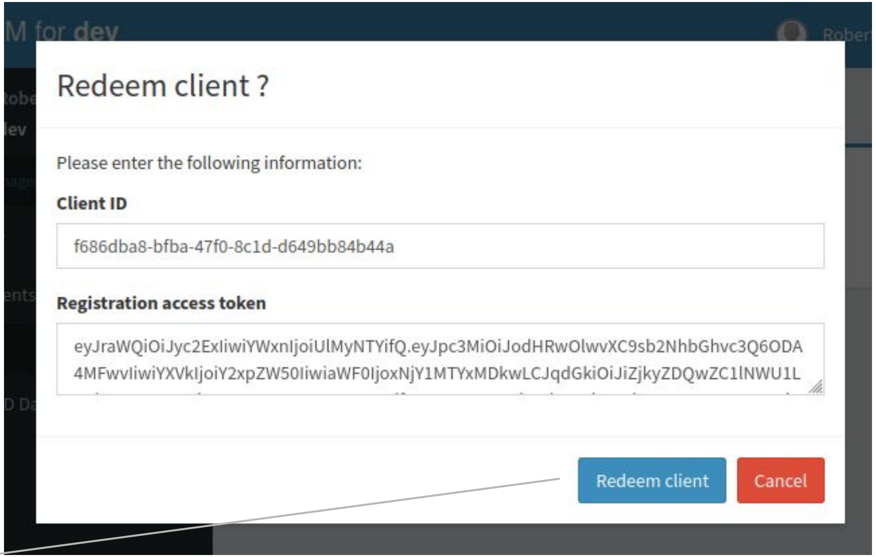
List of email address contacts for administrators of this client

✖ roberta.miccoli@cnaf.infn.it

Refactored client management & registration (6/6)



No clients found.



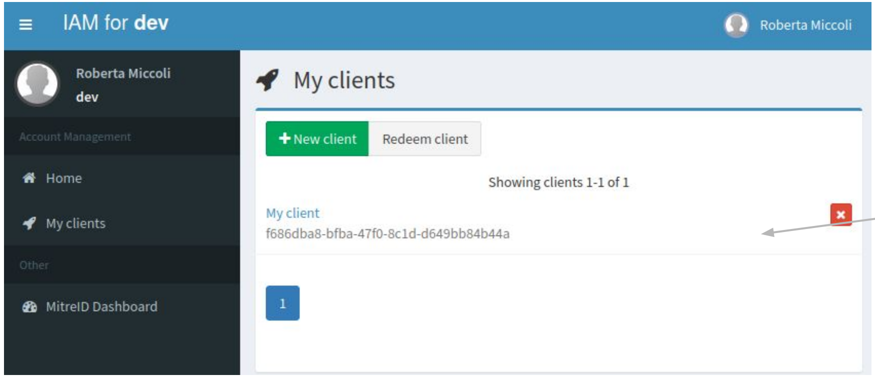
Please enter the following information:

Client ID

f686dba8-bfba-47f0-8c1d-d649bb84b44a

Registration access token

eyJraWQiOiJyc2ExIiwiYWxnIjoiUlMyNTYifQ.eyJpc3MiOiJodHRwOlwvXC9sb2NhbGhvc3Q6ODA
4MFwvIiwiYXVkIjoiY2xpZW50IiwiaWF0IjoxNjY1MTYxMDkwLCJqdGkiOiJiZjkyZDQwZC1lNWU1L



Showing clients 1-1 of 1

My client
f686dba8-bfba-47f0-8c1d-d649bb84b44a

Using JWTs for Client AuthN

From Section 2.2 of RFC 7523: To use a JWT Bearer Token for client authentication, the client uses the following parameter values and encodings:

- The value of the "**client_assertion_type**" is "urn:ietf:params:oauth:client-assertion-type:jwt-bearer".
- The value of the "**client_assertion**" parameter contains a single JWT.
  It MUST NOT contain more than one JWT.
- The request may have the “**scope**” request parameter.

```
POST /token HTTP/1.1
  Host: iam.local.io
  Content-Type: application/x-www-form-urlencoded

  grant_type=client_credentials&
  client_assertion_type=urn%3Aietf%3Aparams%3Aoauth%3A
  client-assertion-type%3Ajwt-bearer&
  client_assertion=eyJhbGciOiJSUzI1NiIsImtpZCI6IjIyIn0.eyJpc3Mi[...omitted for
brevity...].cC4hiUPo[...omitted for brevity...]
```

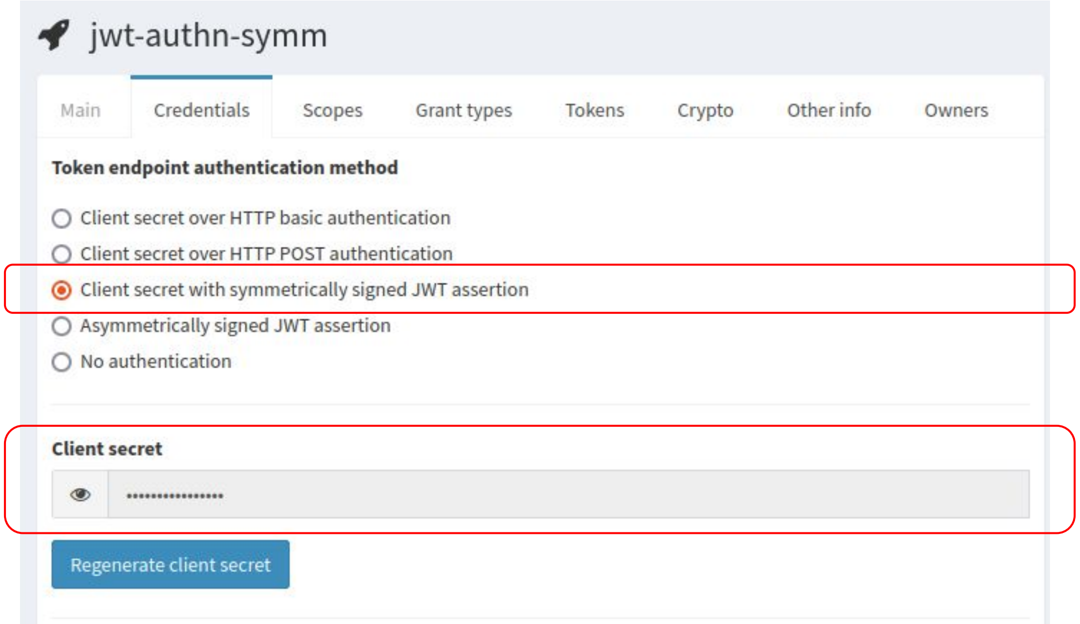
Using JWTs for Client AuthN in INDIGO IAM (1/3)

In INDIGO IAM users can choose between two types of JWT assertion:

- a **symmetrically-signed JWT assertion**, signed with the client_secret
- an **asymmetrically-signed JWT assertion,** signed with a RSA private key
    - IAM can get the RSA public key used to validate the JWT assertion from a JSON Web Keyset that can be provided:
        - by URI
        - by value

Using JWTs for Client AuthN in INDIGO IAM (2/3)

Symmetrically-signed JWT assertion



jwt-authn-symm

Token endpoint authentication method

○ Client secret over HTTP basic authentication

○ Client secret over HTTP POST authentication

● Client secret with symmetrically signed JWT assertion

○ Asymmetrically signed JWT assertion

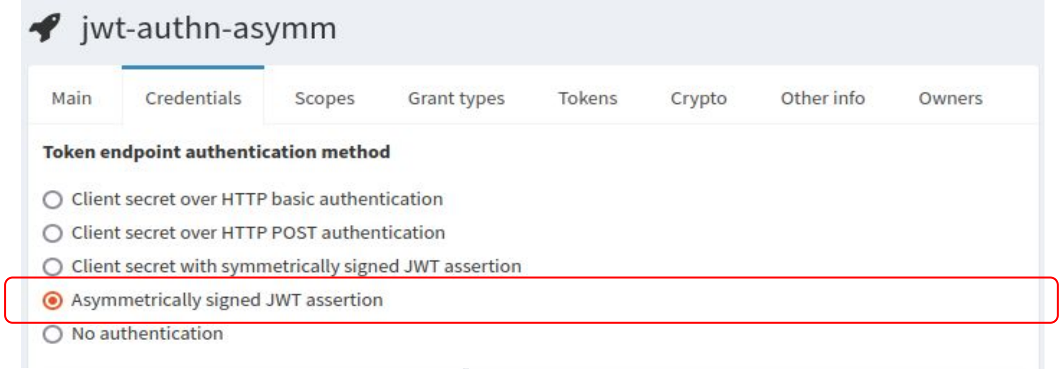
○ No authentication

Client secret

••••••••••••••••

Using JWTs for Client AuthN in INDIGO IAM (3/3)

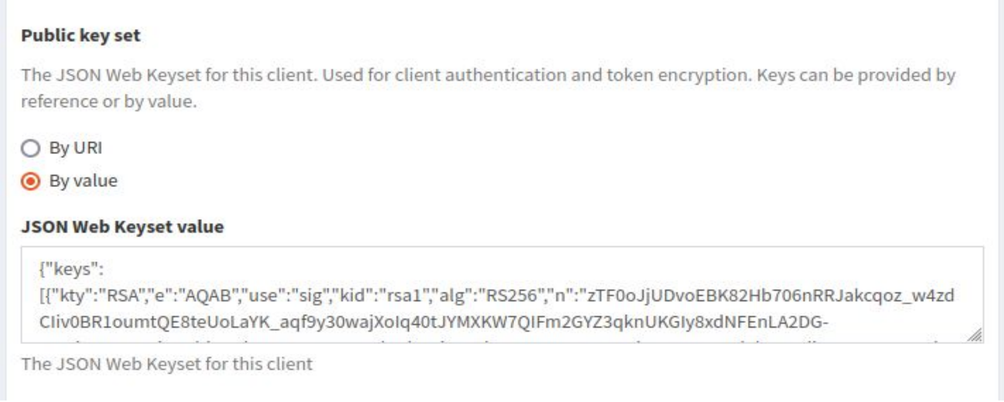
Asymmetrically-signed with a RSA private key



jwt-authn-asymm

Token endpoint authentication method

○ Client secret over HTTP basic authentication
○ Client secret over HTTP POST authentication
○ Client secret with symmetrically signed JWT assertion
● Asymmetrically signed JWT assertion
○ No authentication



Public key set

The JSON Web Keyset for this client. Used for client authentication and token encryption. Keys can be provided by reference or by value.

○ By URI
● By value

JSON Web Keyset value

```
{"keys":
[{"kty":"RSA","e":"AQAB","use":"sig","kid":"rsa1","alg":"RS256","n":"zTF0oJjUDvoEBK82Hb706nRRJakcqoz_w4zd
CIiv0BR1oumtQE8teUoLaYK_aqf9y30wajXoIq40tJYMXKW7QIFm2GYZ3qknUKGIy8xdNFEnLA2DG-
```

The JSON Web Keyset for this client

The JSON Web Keyset can be provided:

- by URI
- by value

How to generate a valid JSON Web Keyset

To generate a JSON Web Keyset you can use the json-web-key-generator tool (example here).

```
java -jar json-web-key-generator.jar -t RSA -s 2048 -i 1 -u sig -S
```

This JWK generator outputs a JSON object similar to this:

```
{
  "keys": [
    {
      "d": "Y5ULK-bLRqKAg6FcuDx4HCQmnMYUv67IQ394KBmw6F-LbdbMhNyn6UH2RAr4Wkg-TL0QX…",
      "e": "AQAB",
      "n": "j37Y-Fmx2Pr9xCHXhBWvDRaXobvpikF2Nd2J_FoK8U5SlMebmqrEwddegw4OoWbBcTfc…",
      "kty": "RSA",
      "use": "sig",
      "kid": "1"
    }
  ]
}
```

How to encode/generate the assertion (1/2)

Helpful site: https://dinochiesa.github.io/jwt/ :)

Example of symmetrically signed decoded assertion:

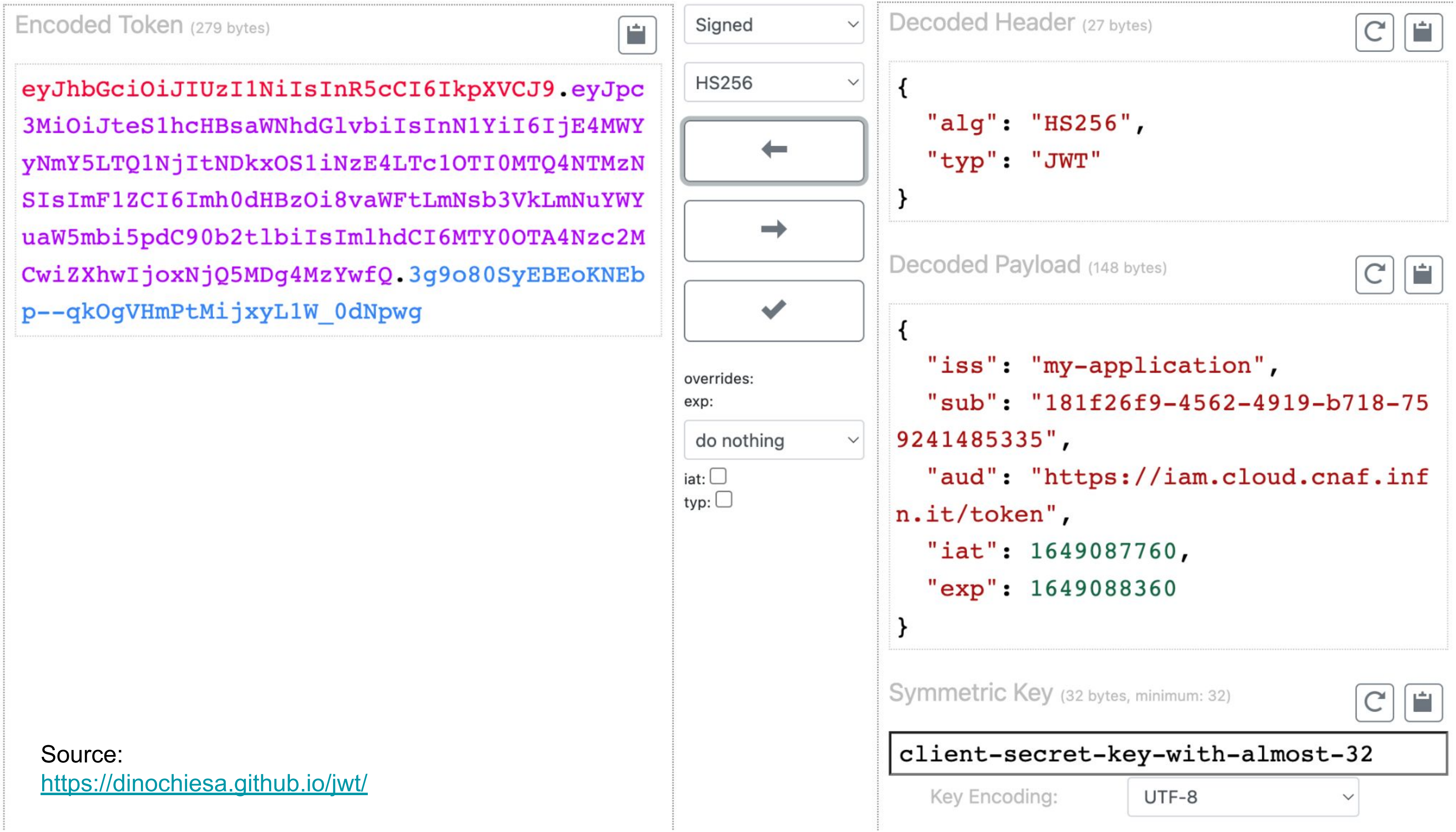
```
## Header
{
  "alg": "HS256"
}
## Payload
{
  "sub": "181f26f9-4562-4919-b718-759241485335",
  "aud": "https://iam.local.io/token",
  "nbf": 1649162752,
  "iss": "181f26f9-4562-4919-b718-759241485335",
  "exp": 1651754752,
  "iat": 1649162752,
  "jti": "120240aa-e389-4a55-8384-f4d7a54c2633"
}
```

How to encode/generate the assertion (2/2)

Helpful site: https://dinochiesa.github.io/jwt/ :)

Example of asymmetrically signed decoded assertion:

```
## Header
{
  "alg": "RS256",
  "kid": "rsa1"
}
## Payload
{
  "sub": "bdb6ca15-be9c-470a-81dc-69d30dabb340",
  "aud": "https://iam.local.io/token",
  "nbf": 1649162752,
  "iss": "bdb6ca15-be9c-470a-81dc-69d30dabb340",
  "exp": 1651754752,
  "iat": 1649162752,
  "jti": "f4392c1e-6d6a-423e-8e5e-5d114585f750"
}
```



Encoded Token (279 bytes)

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJpc
3MiOiJteS1hcHBsaWNhdGlvbiIsInN1YiI6IjE4MWY
yNmY5LTQ1NjItNDkxOS1iNzE4LTc1OTI0MTQ4NTMzN
SIsImF1ZCI6Imh0dHBzOi8vaWFtLmNsb3VkLmNuYWY
uaW5mbi5pdC90b2tlbiIsImlhdCI6MTY0OTA4Nzc2M
CwiZXhwIjoxNjQ5MDg4MzYwfQ.3g9o80SyEBEoKNEb
p--qkOgVHmPtMijxyL1W_0dNpwg
```

overrides:
exp: do nothing
iat: □
typ: □

Decoded Header (27 bytes)

```
{
  "alg": "HS256",
  "typ": "JWT"
}
```

Decoded Payload (148 bytes)

```
{
  "iss": "my-application",
  "sub": "181f26f9-4562-4919-b718-75
9241485335",
  "aud": "https://iam.cloud.cnaf.inf
n.it/token",
  "iat": 1649087760,
  "exp": 1649088360
}
```

Symmetric Key (32 bytes, minimum: 32)

```
client-secret-key-with-almost-32
```

Key Encoding: UTF-8

Source:
https://dinochiesa.github.io/jwt/

JWT-based client authentication

Example of an HTTP POST request to the token endpoint where the client is authenticated with **JWT assertion** and is authorized via the **client credentials** OAuth2 flow.

```
$ export JWTA=eyJhbGciOiJI[...]I6IkpXVCJ9.eyJpc3[...]wfQ.3g9o80SyE[...]W_0dNpwg
$ curl -d client_assertion=${JWTA} -d
client_assertion_type=urn:ietf:params:oauth:client-assertion-type:jwt-bearer -d
grant_type=client_credentials -d scope=storage.read:/ https://iam.local.io/token | jq

{
  "access_token": "eyJraWQiOiJyc2ExIiwiY...",
  "token_type": "Bearer",
  "expires_in": 3599,
  "scope": "storage.read:/"
}
```

Support for AARC guidelines (1/2)

The support of AARC-G002/AARC-G069 guidelines was already included within INDIGO IAM. These guidelines describe how to encode group membership information, in particular:

- groups are not included by default in access and ID tokens
- groups can be requested using the `eduperson_entitlement` scope and they are encoded as URN in the `eduperson_entitlement` claim

Example:

```
$ oidc-token -s eduperson_entitlement aarc-client | cut -d. -f2 | base64 -d
2>/dev/null | jq
{
…
"eduperson_entitlement": [
    "urn:geant:projectescape.eu:group:escape:cms",
    "urn:geant:projectescape.eu:group:escape"
  ]
}
```

In the context of the ESCAPE project, `projectescape.eu`is a delegated namespace registered under *geant*.

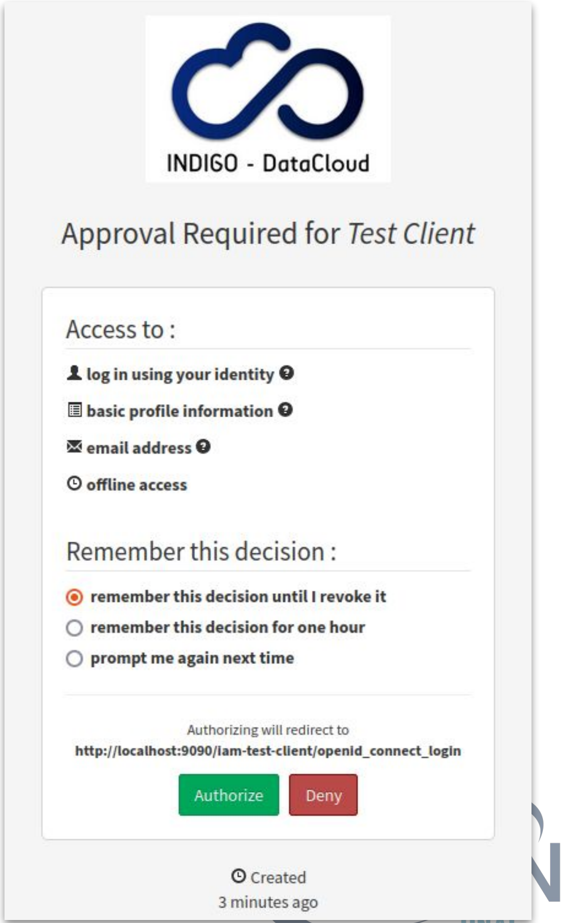
Support for AARC guidelines (2/2)

With IAM v1.8.0, we have added support for two new guidelines to be compliant with AARC BPA

- AARC-G021 for expressing assurance information
  - LoA can be requested using the `eduperson_assurance` scope and it is encoded in the `eduperson_assurance` claim
  - e.g. `"eduperson_assurance": ["https://refeds.org/assurance","https://refeds.org/assurance/IAP/low"]`
- AARC-G025 for expressing affiliation information within Community
  - Affiliation can be requested using the `eduperson_scoped_affiliation` scope and it is encoded in the `eduperson_scoped_affiliation` claim
  - e.g. `"eduperson_scoped_affiliation": "member@projectescape.eu"`

New consent page

- Migrated away from MITREid Connect
- Scopes are now evaluated before prompting the consent page to the user, then:
  - users are no longer asked to authorize scopes they are not authorized to get
  - the consent page shows only the scopes allowed to the user



Approval Required for *Test Client*

Access to :

- log in using your identity
- basic profile information
- email address
- offline access

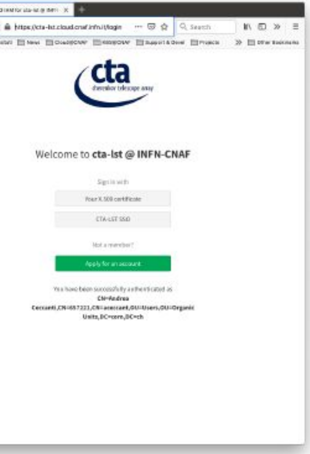
Remember this decision :

● remember this decision until I revoke it
○ remember this decision for one hour
○ prompt me again next time

Authorizing will redirect to
http://localhost:9090/iam-test-client/openid_connect_login

Created
3 minutes ago

INDIGO IAM deployments



https://cta-lst.cloud.cnaf.infn.it/login

Welcome to **cta-lst @ INFN-CNAF**

Sign in with

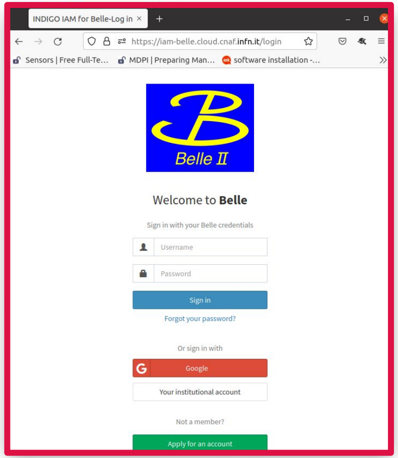
Your X.509 certificate

CTA-LST SSO

Not a member?

Apply for an account

You have been successfully authenticated as **CN=Andrea Ceccanti,CN=657121,CN=aceccant,OU=Users,OU=Organic Units,DC=cern,DC=ch**



INDIGO IAM for Belle-Log in

https://iam-belle.cloud.cnaf.infn.it/login

Sensors | Free Full-Te... MDPI | Preparing Man... software installation -...

Welcome to **Belle**

Sign in with your Belle credentials

Username

Password

Sign in

Forgot your password?

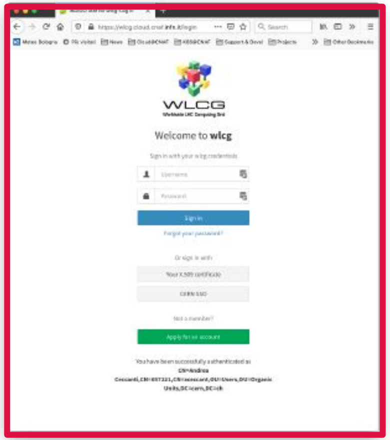
Or sign in with

Google

Your institutional account

Not a member?

Apply for an account



https://wlcg.cloud.cnaf.infn.it/login

Welcome to **wlcg**

Sign in with your wlcg credentials

Username

Password

Sign in

Forgot your password?

Or sign in with

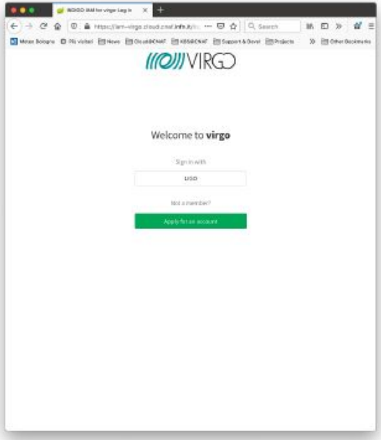
Your X.509 certificate

CERN SSO

Not a member?

Apply for an account

You have been successfully authenticated as **CN=Andrea Ceccanti,CN=657121,CN=aceccant,OU=Users,OU=Organic Units,DC=cern,DC=ch**



INDIGO IAM for virgo-Log in

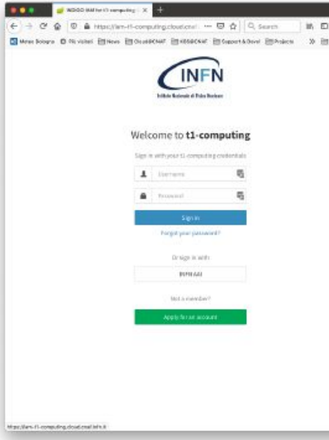
Welcome to **virgo**

Sign in with

SSO

Not a member?

Apply for an account



INDIGO IAM for t1-computing

Welcome to **t1-computing**

Sign in with your t1-computing credentials

Username

Password

Sign in

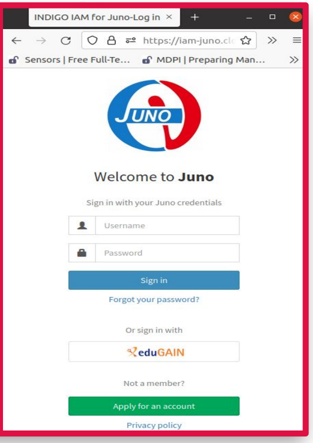
Forgot your password?

Or sign in with

INFN AAI

Not a member?

Apply for an account



INDIGO IAM for Juno-Log in

https://iam-juno.cl

Sensors | Free Full-Te... MDPI | Preparing Man...

Welcome to **Juno**

Sign in with your Juno credentials

Username

Password

Sign in

Forgot your password?

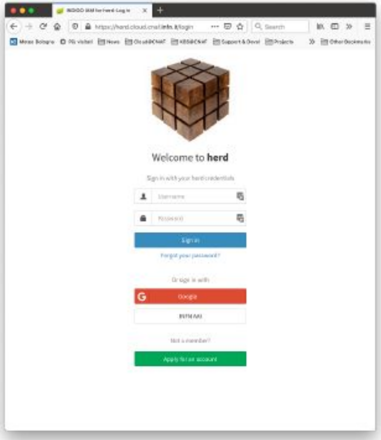
Or sign in with

eduGAIN

Not a member?

Apply for an account

Privacy policy



INDIGO IAM for herd-Log in

https://herd.cloud.cnaf.infn.it/login

Welcome to **herd**

Sign in with your herd credentials

Username

Password

Sign in

Forgot your password?

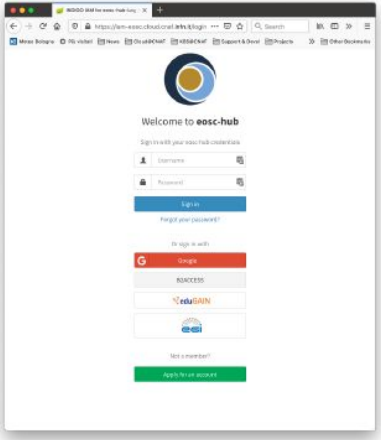
Or sign in with

Google

INFN AAI

Not a member?

Apply for an account



INDIGO IAM for eosc-hub-Log in

https://iam-eosc.cloud.cnaf.infn.it/login

Welcome to **eosc-hub**

Sign in with your eosc-hub credentials

Username

Password

Sign in

Forgot your password?

Or sign in with

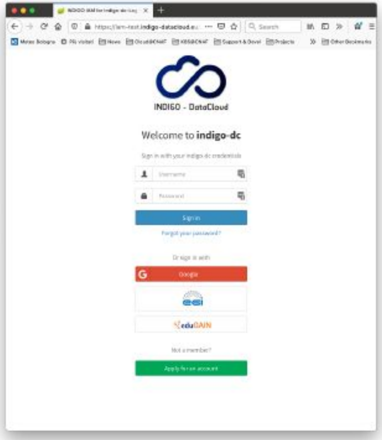
Google

B2ACCESS

eduGAIN

Not a member?

Apply for an account



INDIGO IAM for indigo-dc-Log in

https://iam-test.indigo-datacloud.eu

INDIGO - DataCloud

Welcome to **indigo-dc**

Sign in with your indigo-dc credentials

Username

Password

Sign in

Forgot your password?

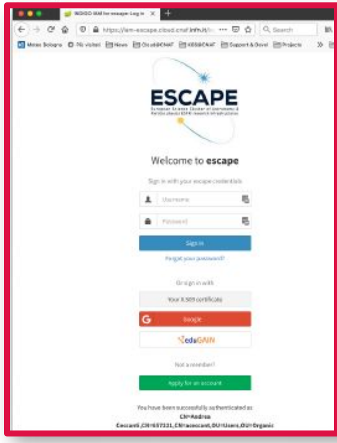
Or sign in with

Google

eduGAIN

Not a member?

Apply for an account



INDIGO IAM for escape-Log in

https://iam-escape.cloud.cnaf.infn.it/

ESCAPE

Welcome to **escape**

Sign in with your escape credentials

Username

Password

Sign in

Forgot your password?

Or sign in with

Your X.509 certificate

Google

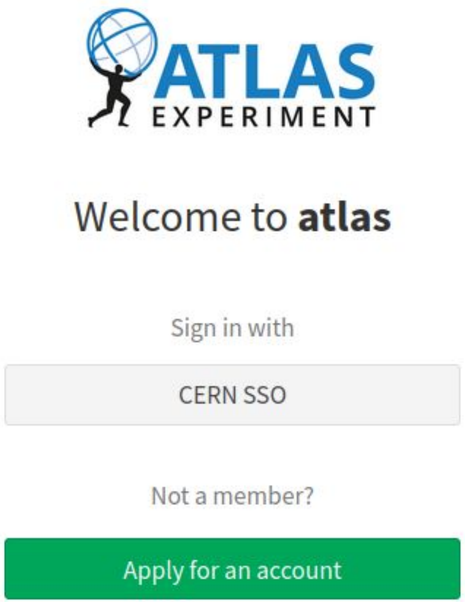
eduGAIN

Not a member?

Apply for an account

You have been successfully authenticated as **CN=Andrea Ceccanti,CN=657121,CN=aceccant,OU=Users,OU=Organic**

WLCG IAM deployments



Welcome to **atlas**

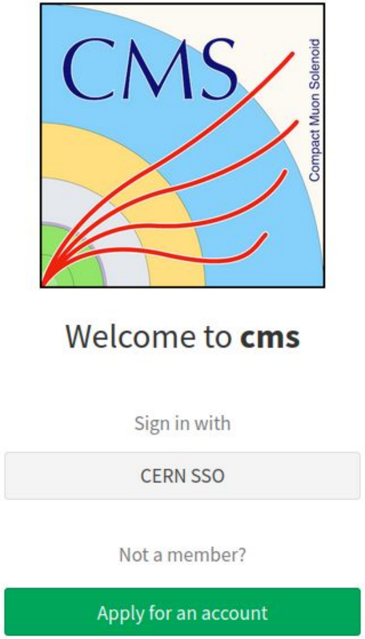
Sign in with

CERN SSO

Not a member?

Apply for an account

atlas-auth.web.cern.ch/



Welcome to **cms**

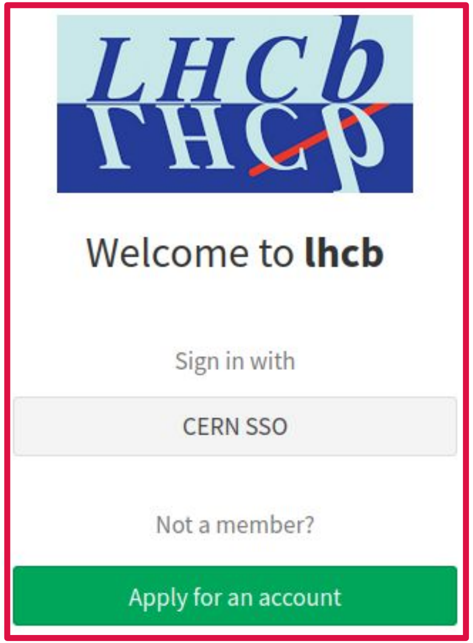
Sign in with

CERN SSO

Not a member?

Apply for an account

cms-auth.web.cern.ch/



Welcome to **lhcb**

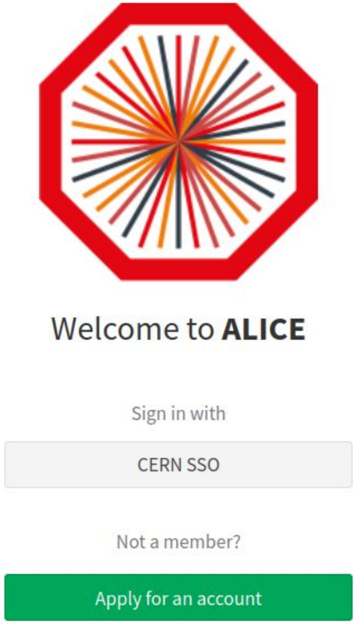
Sign in with

CERN SSO

Not a member?

Apply for an account

lhcb-auth.web.cern.ch/



Welcome to **ALICE**

Sign in with

CERN SSO

Not a member?

Apply for an account

alice-auth.web.cern.ch/

INDIGO IAM - future developments

Planned release: IAM v1.8.1

To-Be-Added:

- Add scope policy management into IAM dashboard #382
- Migrate scope management to IAM dashboard #85
- Improve support for AARC guidelines

To-Be-Fixed:

- IAM VOMS attribute authority should not issue attribute certificates to users with an expired AUP signature #446
- IAM should not allow token refresh for users with an expired AUP signature #447
- Can't add certificate with same subject and different issuer #454
- IAM should not allow token refresh for disabled users #508
- IAM should issue a new RT when making token refresh flow #509

Planned release: IAM v1.9.0

To-Be-Added:

- Support for HA deployments #436
- Support for Multi-factor Authentication #418

and other remaining open issues

INDIGO IAM - open discussion

- IAM administrators’ tokens give privileges regardless of scopes (e.g. scim:write)
  - can we consider to have a second separate account for VO-Admins ?

- Review the workflow of suspended users

- Why don’t automatically create all ATLAS accounts in IAM according HR database with default list of groups (e.g. /atlas)?
  - user must sign AUP before new account can be used for Grid activities
  - user must register certificate subject to be able to get X.509 VOMS proxy

Source: https://codimd.web.cern.ch/f9aVkBexTXi1xTC5adZP0g?view#

- Do we want association of service accounts with CERN HR personal ID?
  - being able to identify owner

- User can choose IAM username/email (CERN username/email is default suggestion) during registration
  - do we really want to give user such freedom?

- User group request is sent to both - IAM Group Managers and IAM administrators
  - should IAM administrators get all these emails?

- Audit of changes (who / when / what)
  - how to give access to these data

Source: https://codimd.web.cern.ch/f9aVkBexTXi1xTC5adZP0g?view#

"I don't need to worry about identity theft because no one wants to be me."

Jay London

Useful references

IAM on GitHub: https://github.com/indigo-iam/iam

IAM documentation: https://indigo-iam.github.io/docs

IAM in action video: https://www.youtube.com/watch?v=1rZlvJADOnY

For general information:

- OAuth 2.0: https://oauth.net/2/ and OAuth 2.1: https://oauth.net/2.1/
- OpenID Connect: https://openid.net/connect/

Contacts:

- iam-support@lists.infn.it