

INDIGO IAM Community Meeting

October 20th, 2023

Welcome!

This meeting is dedicated to the community of INDIGO IAM developers.

INDIGO IAM has been developing at INFN-CNAF since 2016.

During the last [IAM Hackathon](#) there was the interest about contributing to INDIGO IAM codebase outside INFN-CNAF then we decided to start having a developers “community meeting”.

Everyone who is interested on developing/contributing is welcome!

Round table presentation



Internal communication

How can we communicate?

- Mattermost chat (WLCG IAM developers and also a dedicated channel),
- Github issues
- other?

We have a support mailing list where all developers can support users but can be used by the subscribed to communicate:

iam-support@lists.infn.it ⇒ [subscribe](#)

Meeting frequency

The idea is for a monthly community meeting, but:

- we can have dedicated meeting (for a particular task e.g.)
- we can have another meeting next week if today is not enough to bootstrap contributions
 - or start as a bi-weekly instead

Contributing

Github Organization: <https://github.com/indigo-iam/>

Github INDIGO IAM project: <https://github.com/indigo-iam/iam>

Send us your Github user nickname and you'll be added to **IAM-devs** group, allowed to maintain INDIGO-IAM code.

How to contribute (draft):

<https://github.com/indigo-iam/iam/blob/686e16c24c6a360a3bc78aa5bb1d9ee0df27001e/CONTRIBUTING.md>

How to contribute - Setup

The INDIGO IAM service is a Maven project built with Java 17.

To download the necessary dependencies from the CNAF Repository platform (e.g. to include the patched version of MitreID), use a custom Maven settings file locally, at `~/.m2/settings.xml`.

<https://github.com/italiangrid/build-settings/blob/master/maven/cnaf-mirror-settings.xml>

```
$ mvn clean package -DskipTests
```

How to contribute - Get started

A Java Google style formatter is used to format code.

Eclipse Java Google style formatter

Run INDIGO IAM as a Spring Boot application:

- main class is **it.infn.mw.iam.IamLoginService**
- needed Spring profiles **h2, dev**
- go to <http://localhost:8080/h2-console> to browse the in memory database
- default users **admin** and **test** with password ***password*** are created

How to contribute - Repository workflow

- the **master** branch is the one containing the latest INDIGO IAM released
- the **develop** branch is the one containing the latest release candidate
 - it should always compile (please)
 - no direct development on this (please)
- developments starts from develop branch and on branches possibly named **issue-<number>** in order to keep a reference to the related issue (if there's no issue related evaluate if it's needed or not)
- do all the commits you want ⇒ they'll be squashed before merging on develop
- create a draft Pull Request to develop since the beginning of your developments
 - as soon as it has to be reviewed, remove draft and add someone of the team as a reviewer
 - wait for the GitHub workflow to finish running. If the build succeeds, a Sonar analysis for code quality runs. Please fix spotted problems, if any. We want to keep as much code coverage as possible (a lower threshold is set to 85%), so add JUnit tests to the uncovered parts of your code.

How to contribute - Commits

Even if we will squash all commits of a PR into a unique well described commit, we invite you to follow few these best practices:

- first letter of the commit must be capital
- tenses in the commit must not be past-like
- the first line of the commit must be included within 50 characters. Add a new blank line if you want to add more explanation of your commit (this will make more readable a git log --oneline command output, for instance).

INDIGO IAM v1.8.3 status

INDIGO IAM v1.8.3

[Drafted release notes]

Changed

- Save access token value as an hash in order to use lighter db indexes and avoid conflicts by [@rmiccoli](#) in [#613](#)
- Avoid upper case characters into VO names by [@SteDev2](#) in [#616](#)
- Enable Redis scope matchers and well-known endpoint caching by [@federicaagostini](#) in [#633](#)
- Consider scope matcher based on string equality for custom scopes by [@rmiccoli](#) in [#642](#)

INDIGO IAM v1.8.3

[Drafted release notes]

Added

- Add SCIM endpoint entry to well-known endpoint by [@federicaagostini](#) in [#631](#)
- Update account AUP signature time via API by [@rmiccoli](#) in [#608](#)
- Add new JWT profile that rename 'groups' claim with 'roles' by [@enicovianello](#) in [#637](#)
- Add support for displaying specific language name in federation Metadata by [@Sae126V](#) in [#640](#)
- Add missing "Reuse refresh token" box within client management page by [@rmiccoli](#) in [#650](#)
- Add missing foreign keys to the database by [@enicovianello](#) in [#632](#)
- Add OpenID Connect standard claims in ATs for WLCG JWT profile by [@rmiccoli](#) in [#651](#)

INDIGO IAM v1.8.3

[Drafted release notes]

Fixed

- Allow to add certificates with the same subject DN by [@rmiccoli](#) in [#624](#)
- Delete unsupported response types by [@rmiccoli](#) in [#610](#)
- Fix management of tokens lifetime following RFC9068 by [@federicaagostini](#) in [#620](#)
- Fix CERN Restore workflow by [@hannahshort](#) in [#645](#)
- Fix authz code flow with PKCE for IAM test client application by [@rmiccoli](#) in [#653](#)

INDIGO IAM v1.8.3 - Board

<https://github.com/orgs/indigo-iam/projects/5>

We're testing again and again latest migrations because...

Recommendations

It is strongly recommended to **make a backup of your database before upgrading to v1.8.3** because several migrations are planned. Also, remember that for updates from versions prior to v1.7.2 you must first upgrade to v1.7.2.

The migration to v1.8.3 will take an amount of time which will be proportional to the amount of currently active access tokens. This means that if you are deploying IAM with some kind of liveness and readiness probes, it's probably better to switch them off before upgrading. This migration may take a long time.

INDIGO IAM v1.8.3 - Avoid doing this

<https://codimd.infn.it/CVXriIQRip63nhZSvwqw>

Rollback from a broken upgrade to v1.8.3 to v1.8.2p2:

```
ALTER TABLE access_token DROP INDEX at_tvh_idx;  
ALTER TABLE access_token DROP COLUMN token_value_hash;  
-- Create unique index on token value  
ALTER TABLE access_token add UNIQUE(token_value(766));
```

```
CREATE INDEX atp_idx ON access_token_permissions (access_token_id, permission_id);  
ALTER TABLE access_token_permissions DROP PRIMARY KEY;
```

```
DELETE FROM schema_version WHERE version IN (93, 94, 95, 96);
```

```
ALTER TABLE token_scope DROP FOREIGN KEY FK_token_scope_owner_id;  
ALTER TABLE client_request_uri DROP FOREIGN KEY FK_client_request_uri_owner_id;  
ALTER TABLE client_post_logout_redirect_uri DROP FOREIGN KEY FK_client_post_logout_redirect_uri_owner_id;  
ALTER TABLE client_default_acr_value DROP FOREIGN KEY FK_client_default_acr_value_owner_id;  
ALTER TABLE client_contact DROP FOREIGN KEY FK_client_contact_owner_id;
```

...



Istituto Nazionale di Fisica Nucleare

Assign/plan next tasks

Next steps

Restore MFA work by Sam (STFC)

Migrate to Spring Security ⇒ and no more dependencies on MitreID codebase

Support OIDC Federations

Deployments with one primary instance and secondary instances connected

Geographical distribution of INDIGO IAM (or at least VOMS AA)

New users/admins dashboards to replace AngularJS

More AARC guidelines support

PostgreSQL support

Java code profiling

...

<https://github.com/orgs/indigo-iam/projects/2>

Useful references/presentations

JSON Web Token [RFC 7519](#)

Bearer Token Usage [RFC 6750](#)

The OAuth 2.0 Authorization Framework [RFC 6749](#)

Device Code Grant [RFC 8628](#)

Token Exchange [RFC 8693](#)

Proof of Key Code Exchange [RFC 7636](#)

[INDIGO IAM: current status & future developments](#)

[INDIGO IAM: future developments and OIDC federations](#)

[Introduction to OAuth and its applications](#)

[INDIGO IAM - status and evolution plans](#)

[Status and prospects of WLCG transition to tokens](#)



Next meeting

Friday 27th October

<https://agenda.infn.it/event/38092/>

Homework for the new ones or the ones interested about joining developments:

- subscribe mailing list iam-support@lists.infn.it ⇒ [subscribe](#)
- choose one (or more? :)) topics you're interested
 - from IAM issues <https://github.com/indigo-iam/iam/issues>
 - from the listed activities listed in previous slides
- try to git clone and build/run IAM locally and report problems

Thanks :)