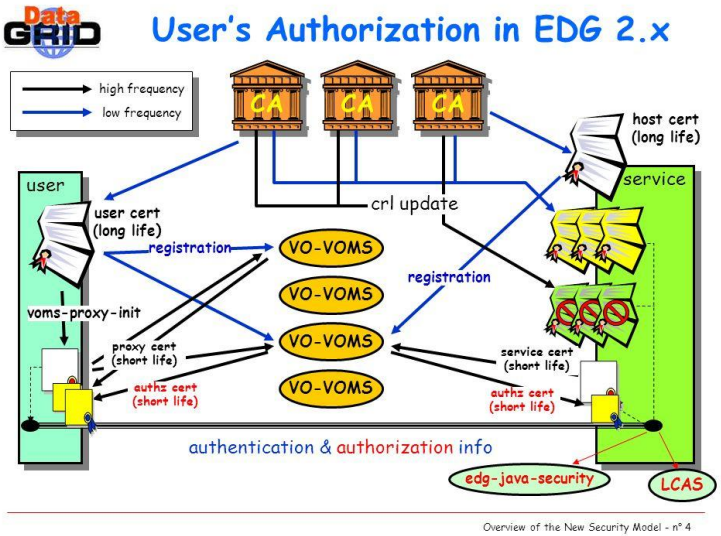
Da proxy VOMS a token: cosa cambia per un VO Admin

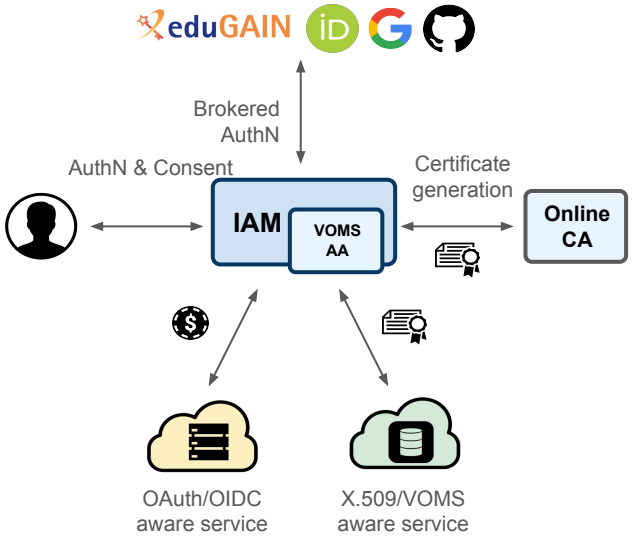
Corso di formazione “Panoramica su OAuth2/OpenID Connect e sue applicazioni tramite il servizio INDIGO IAM”, 12-14 Maggio 2025, LNF

Federica Agostini, INFN CNAF

Evolution of the WLCG AAI beyond X.509



Move beyond X.509



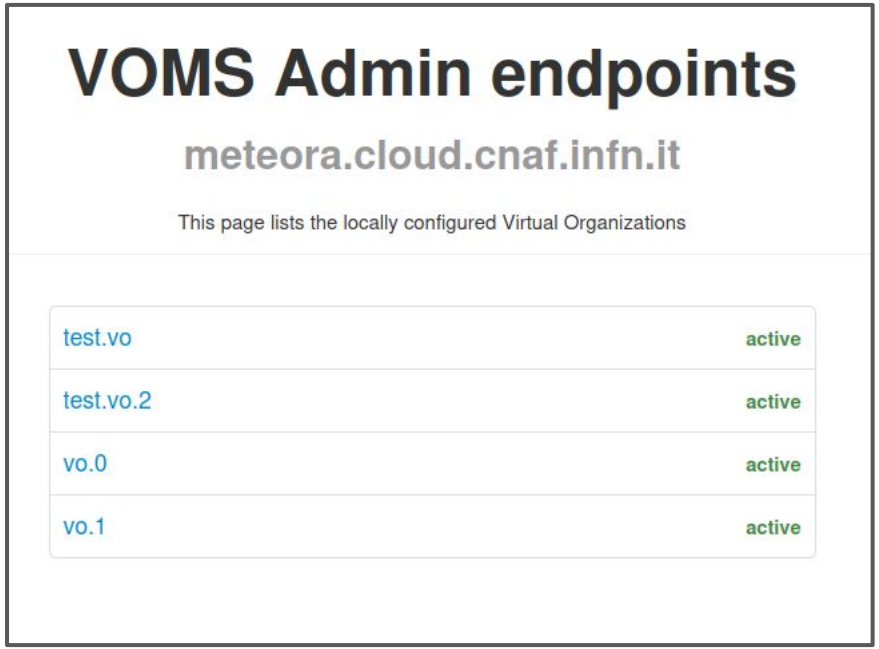
VOMS

In VOMS (*Virtual Organization Membership Access*), a Virtual Organisation is a named container for a set of VO members organized in groups.

VOs are managed by one or more VO Administrators, i.e. privileged users that are responsible for defining the VO structure (groups, roles, attribute), approve user requests and perform other administrative tasks

In this example, 4 VOs are served by VOMS

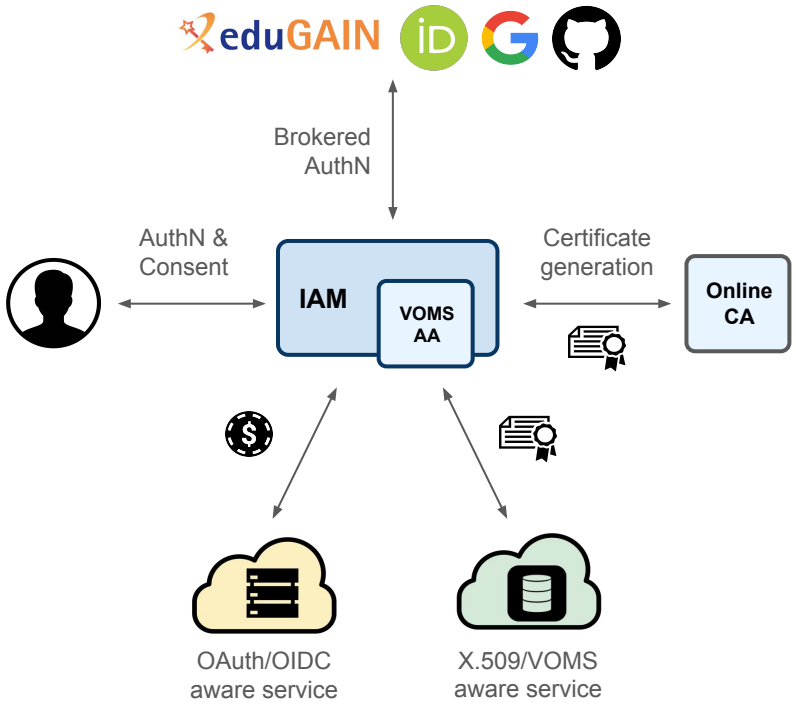
- test.vo
- test.vo.2
- vo.0
- vo.1



https://meteora.cloud.cnaf.infn.it:8443/

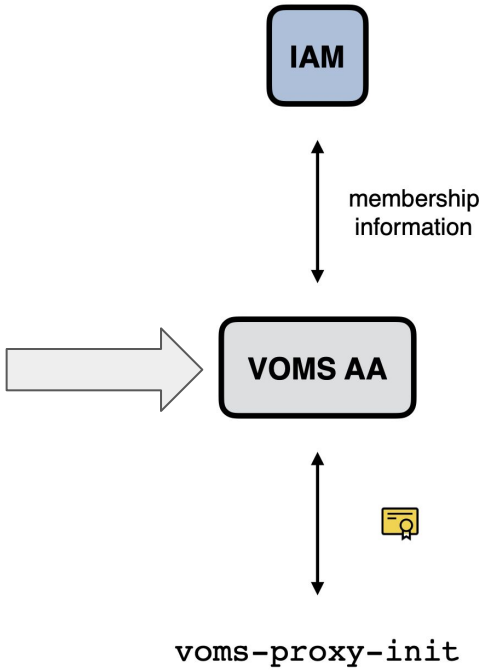
INDIGO IAM

- *Identity and Access Management* (IAM) service
- *Authentication and authorization* service which manages user identities, enrollments, group memberships, etc., for a single Organization
- Supports **multiple authentication mechanisms**, such as username/password, X.509 certificates, OIDC providers (Google, Github, etc.), SAML providers and federations (e.g. EduGAIN)
- Smooth transition from a VOMS-based infrastructure
- Issues **JWT** tokens and VOMS attribute certificates with **identity** and **membership information**, **attributes** and **capabilities** (scopes)



From VOMS to INDIGO IAM

- Knowing that the transition from X.509 to tokens will take time, IAM was designed to be **backward-compatible** with our existing infrastructure
- The INDIGO IAM web interface provides similar functionalities than VOMS Admin
- IAM also **provides a VOMS Attribute Authority** (VOMS-AA) micro-service that may encode IAM membership information in a standard VOMS Attribute Certificate
  - read-only IAM database
  - can issue VOMS credentials (`voms-proxy-init`) understood by existing clients
- Proven compatibility with existing clients and Grid services



Demo:
VO Admin and Group Managers perspective

What will be demonstrated

Manage users

- change user details
- disable/restore users
- assign admin privileges to a user
- sign AUP on behalf of a user and request AUP signature
- reset user’s password and MFA
- add user to a group
- add certificate to a user
- set a user attribute

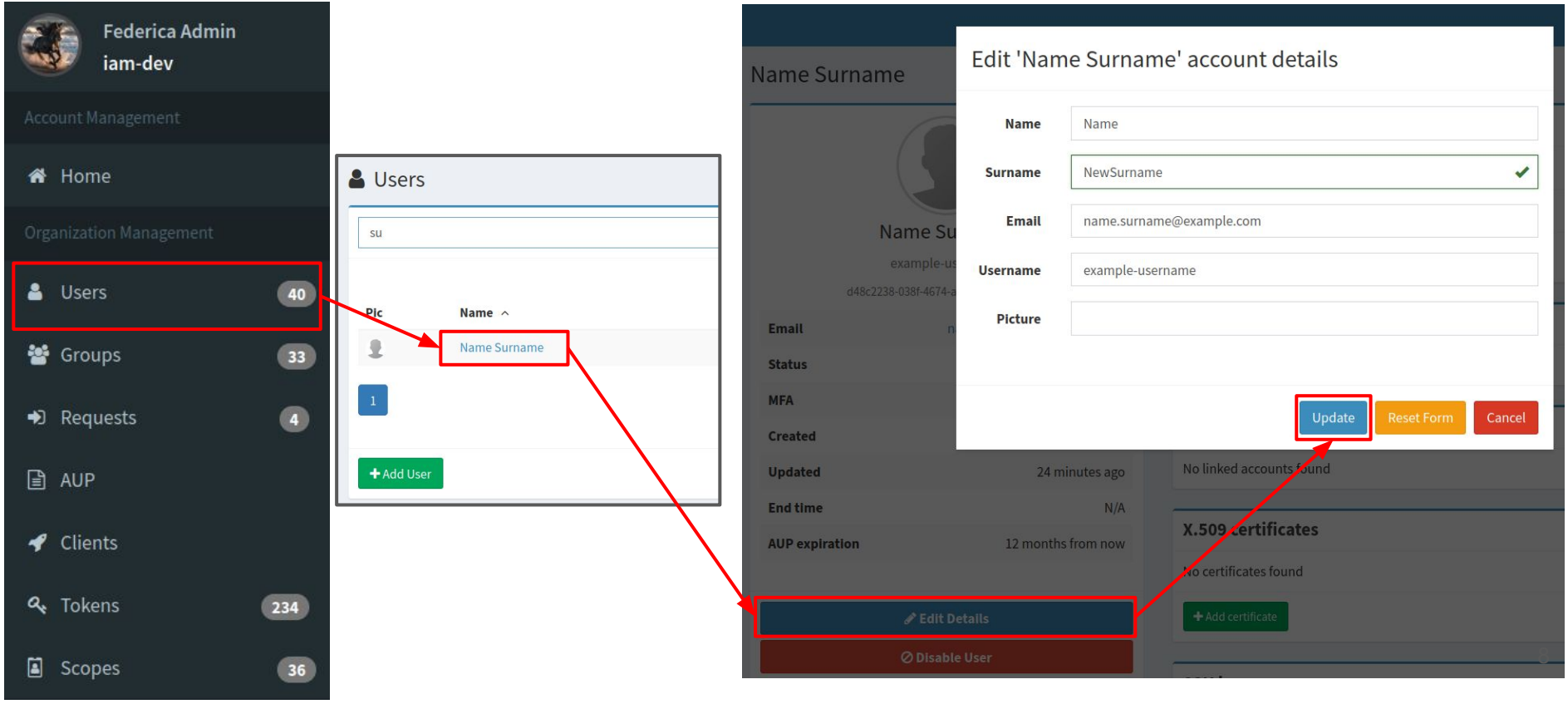
Manage groups

- add optional group
- assign group manager privileges to a user
- approve group membership requests

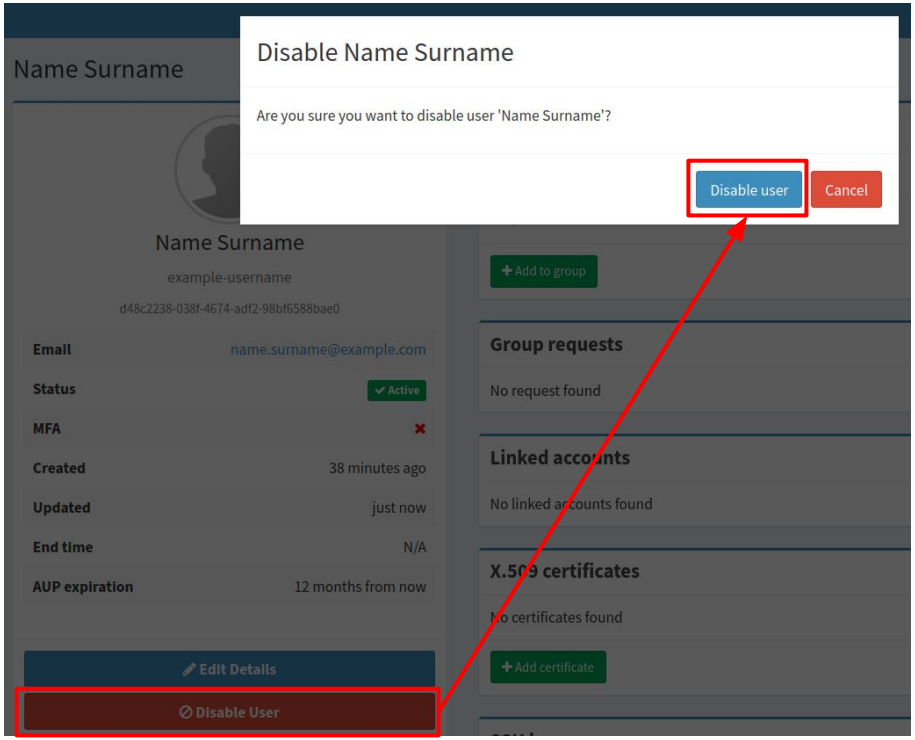
Approve VO membership requests

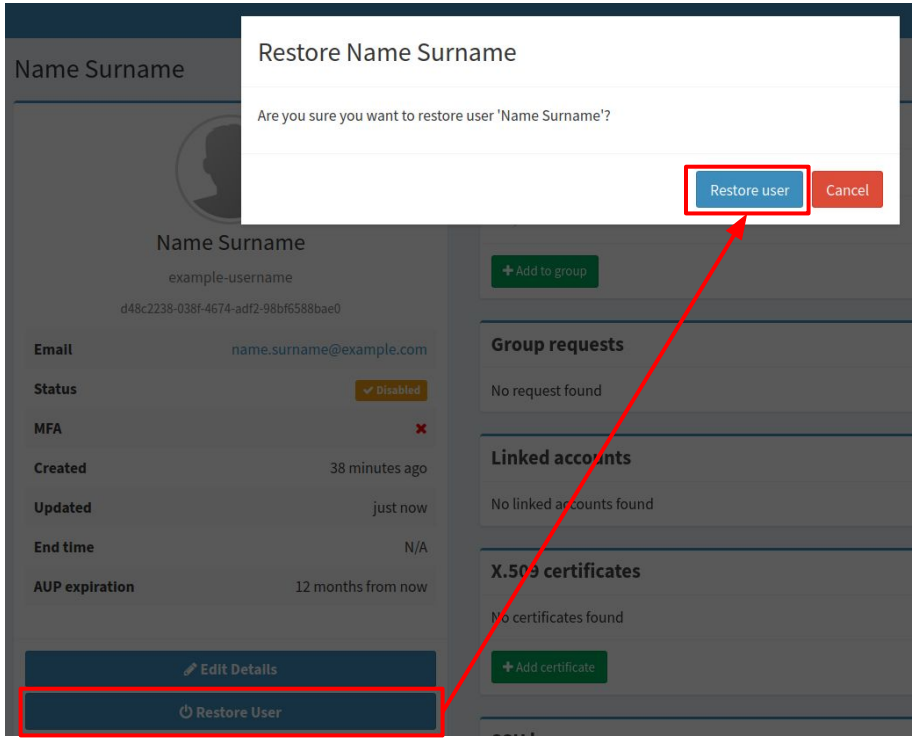
Manage AUP

Manage users: edit details



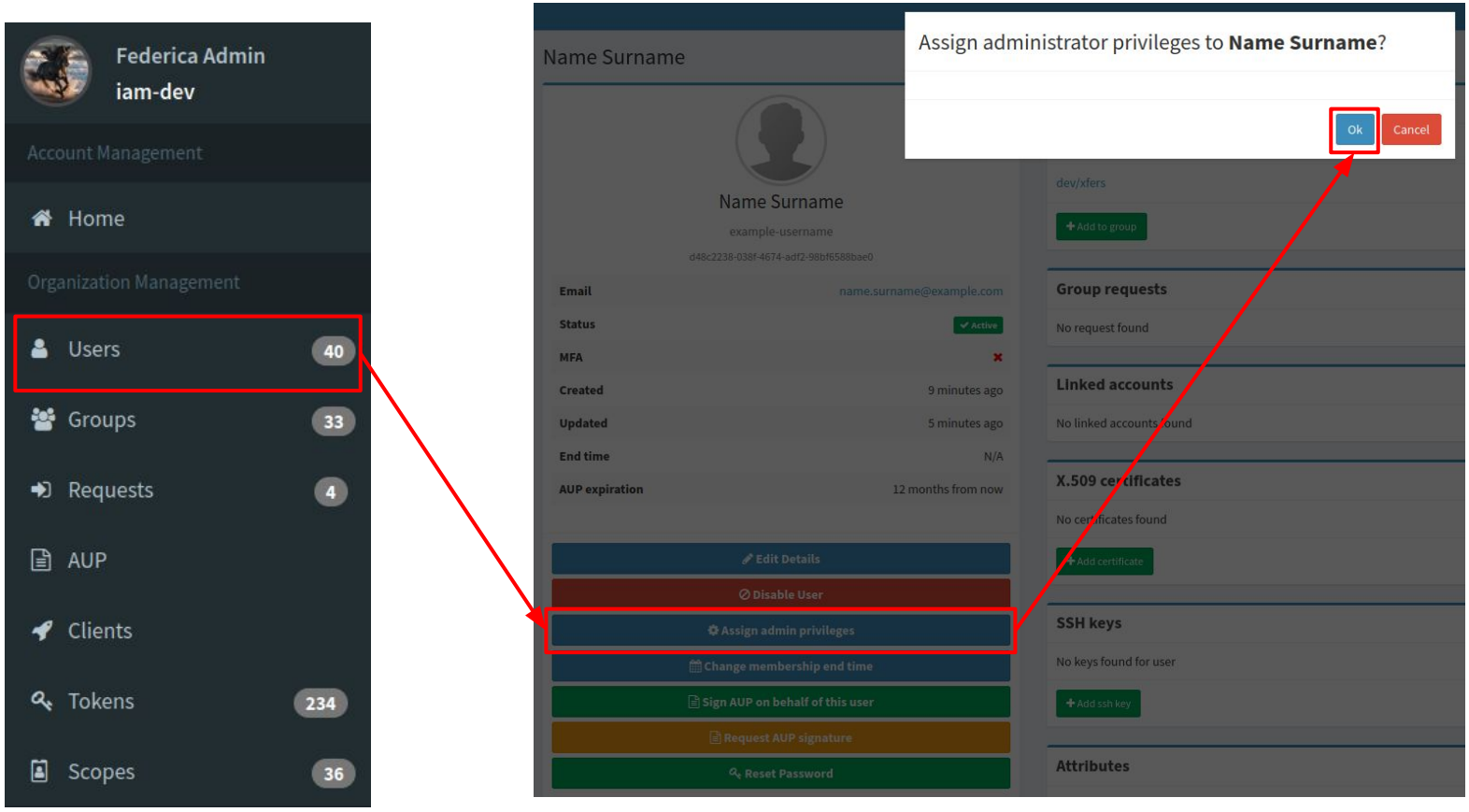
Manage users: disable/restore



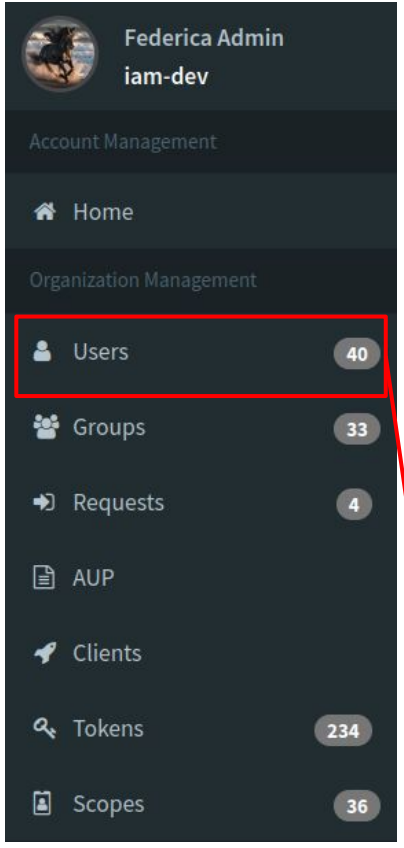


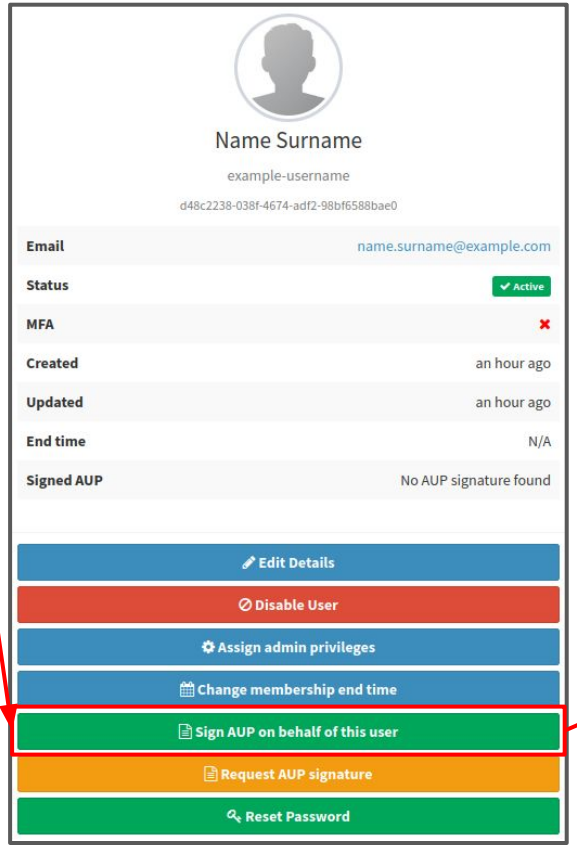
A disabled user cannot login to IAM, obtain access/refresh tokens and VOMS proxies

Manage users: assign admin privileges

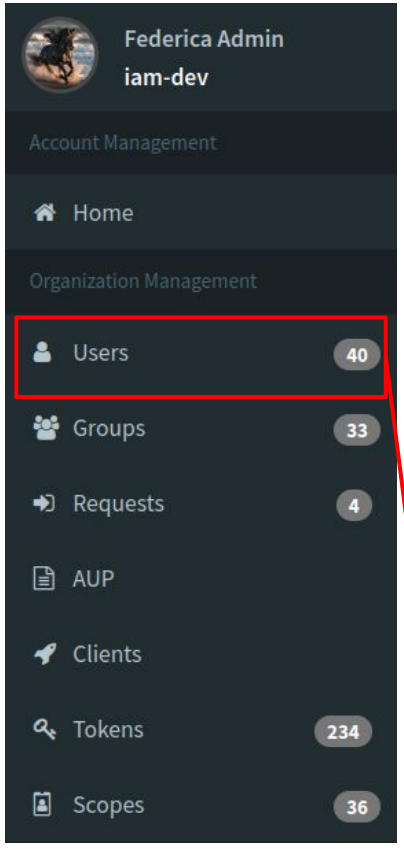


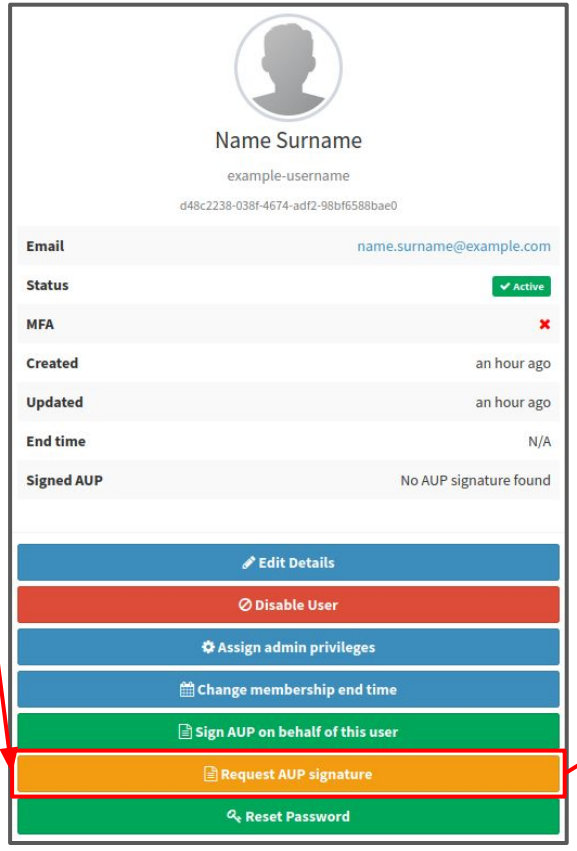
Manage users: sign AUP on they behalf



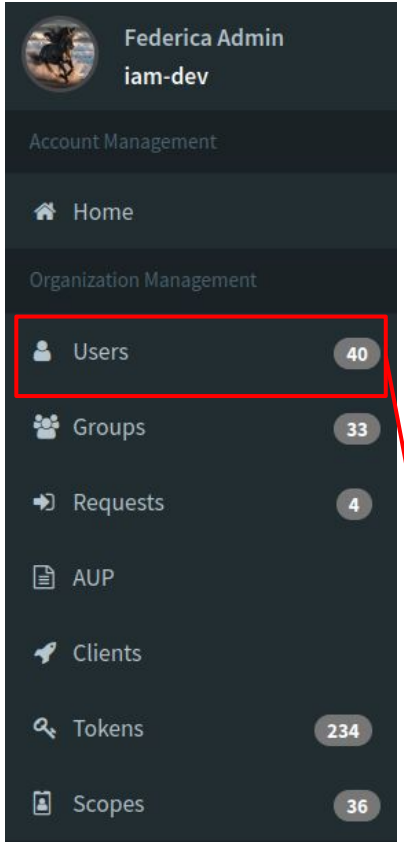


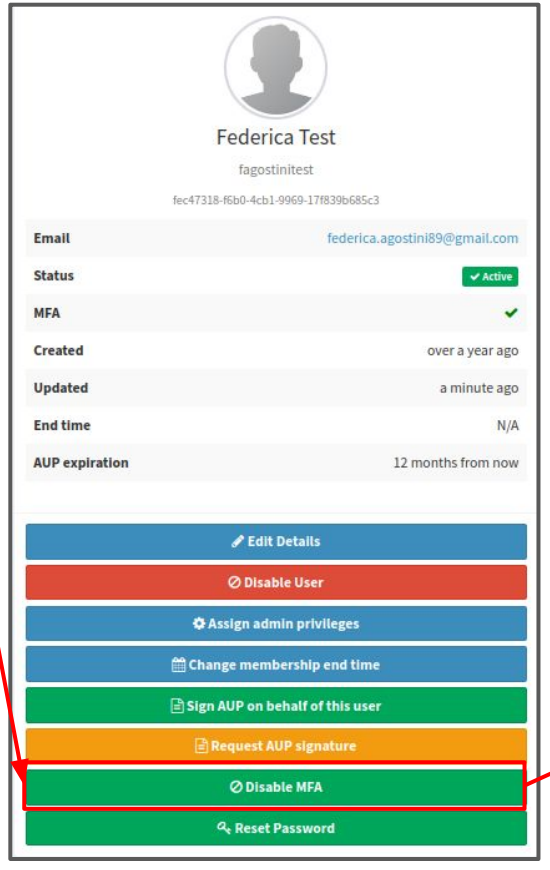
Manage users: request AUP signature





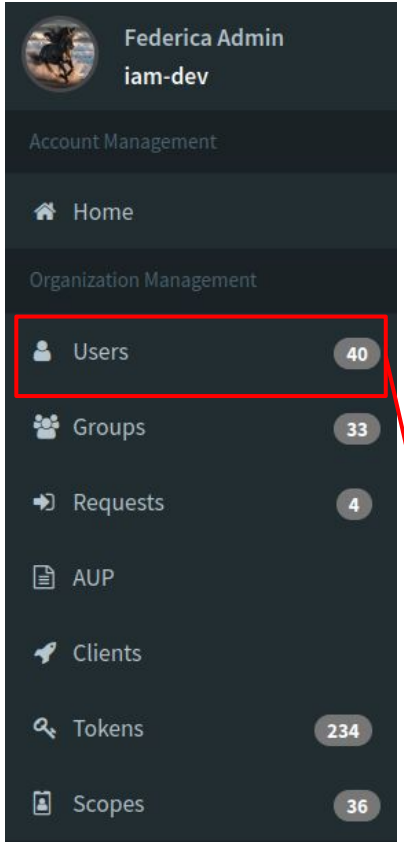
Manage users: disable MFA

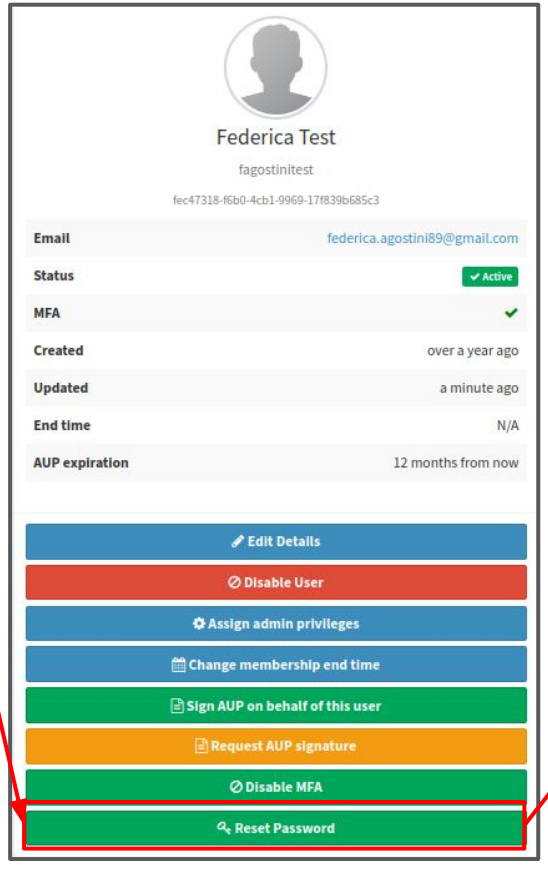


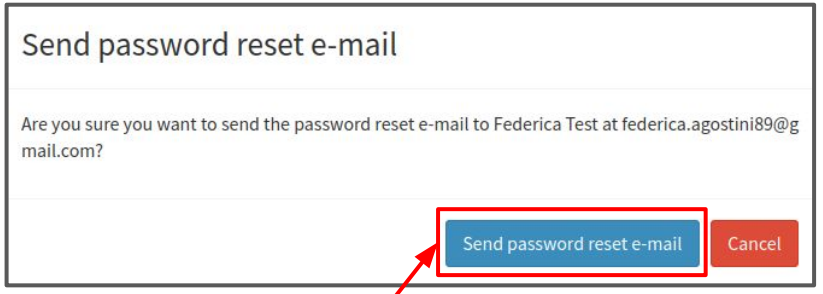


The *Disable MFA* button appears only if the user has enabled MFA for its account

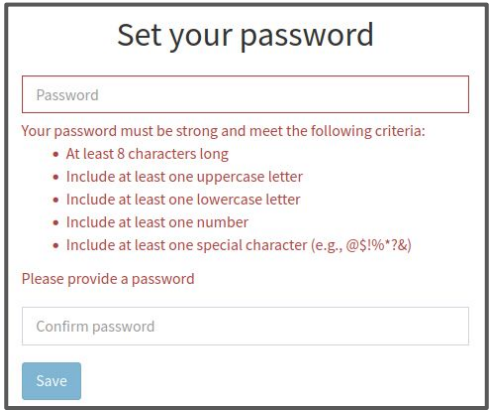
Manage users: reset password



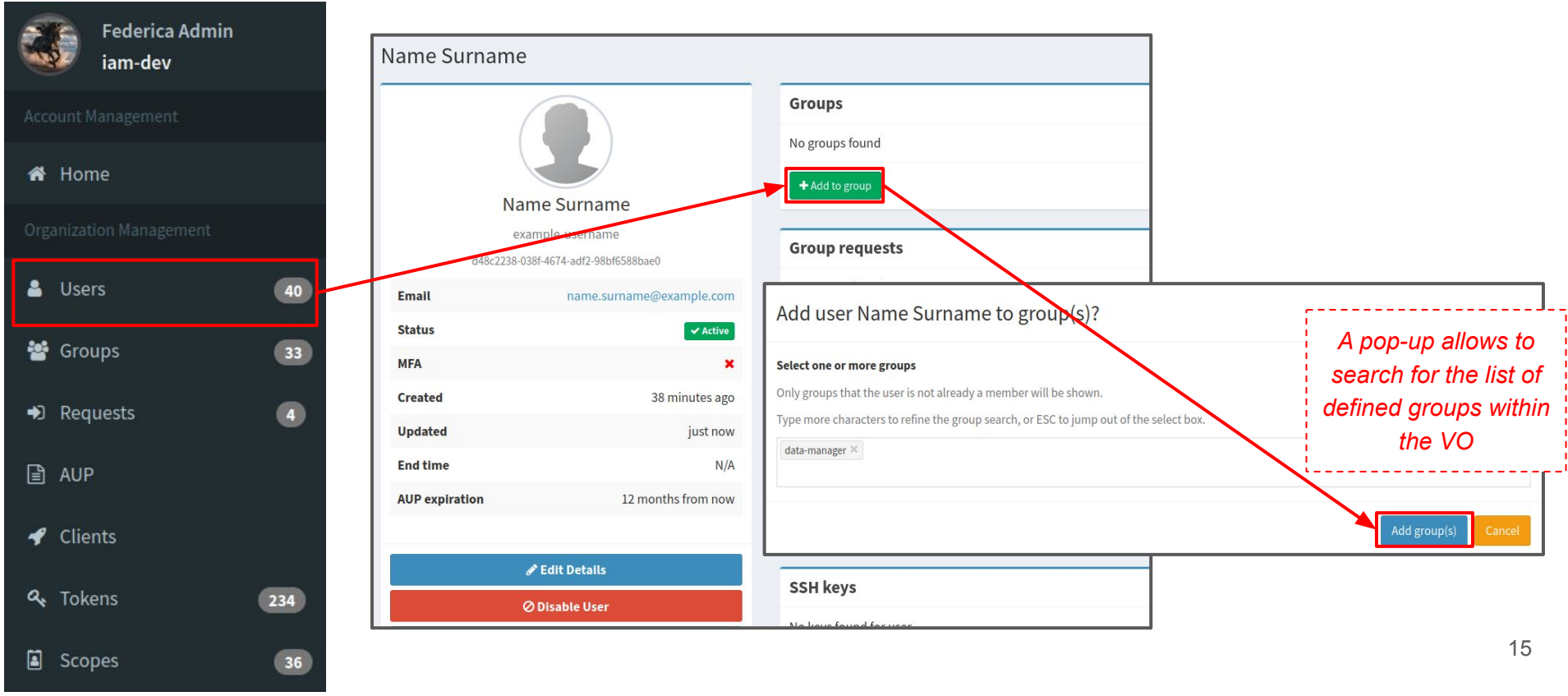




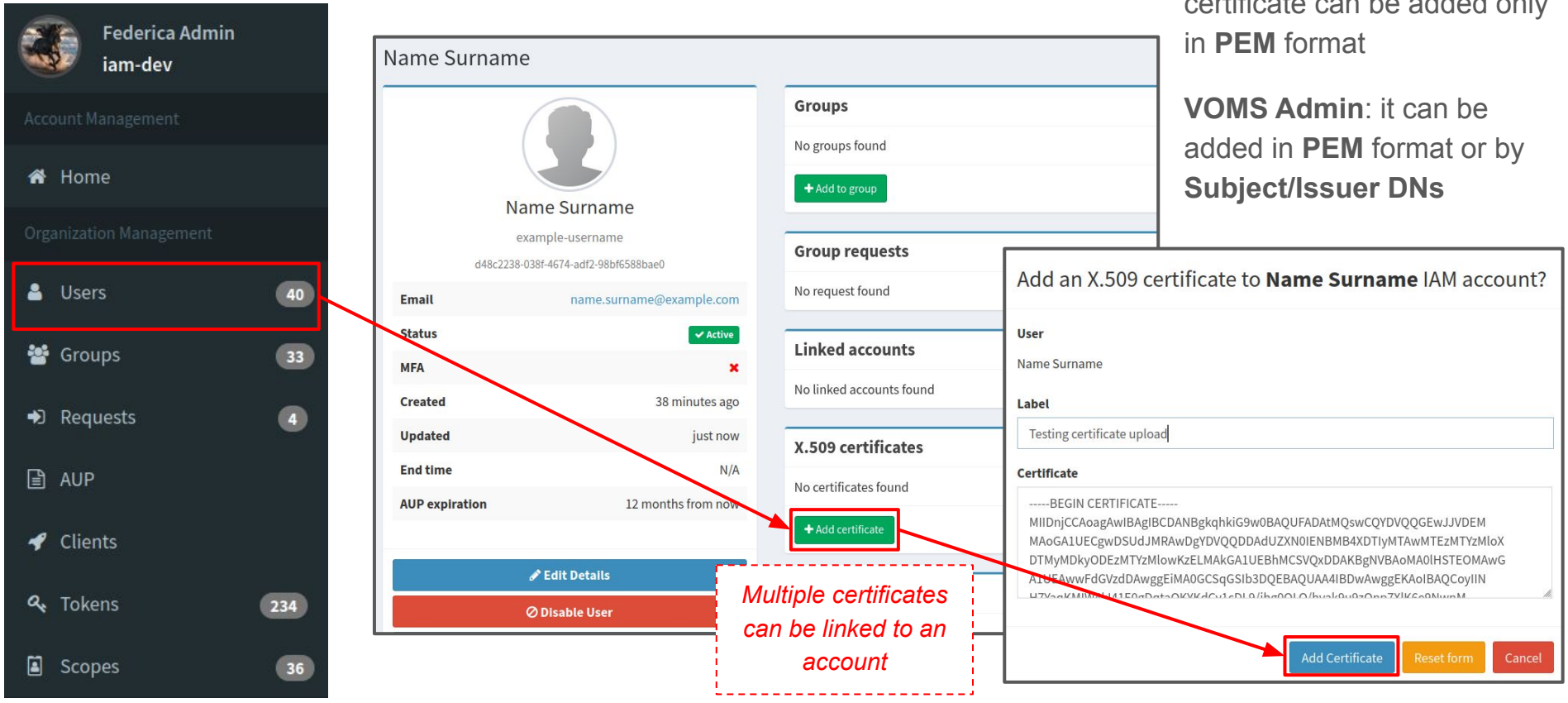
This triggers sending an email to the user with a link for an IAM form which allows to set the new (strong) password



Manage users: add to group



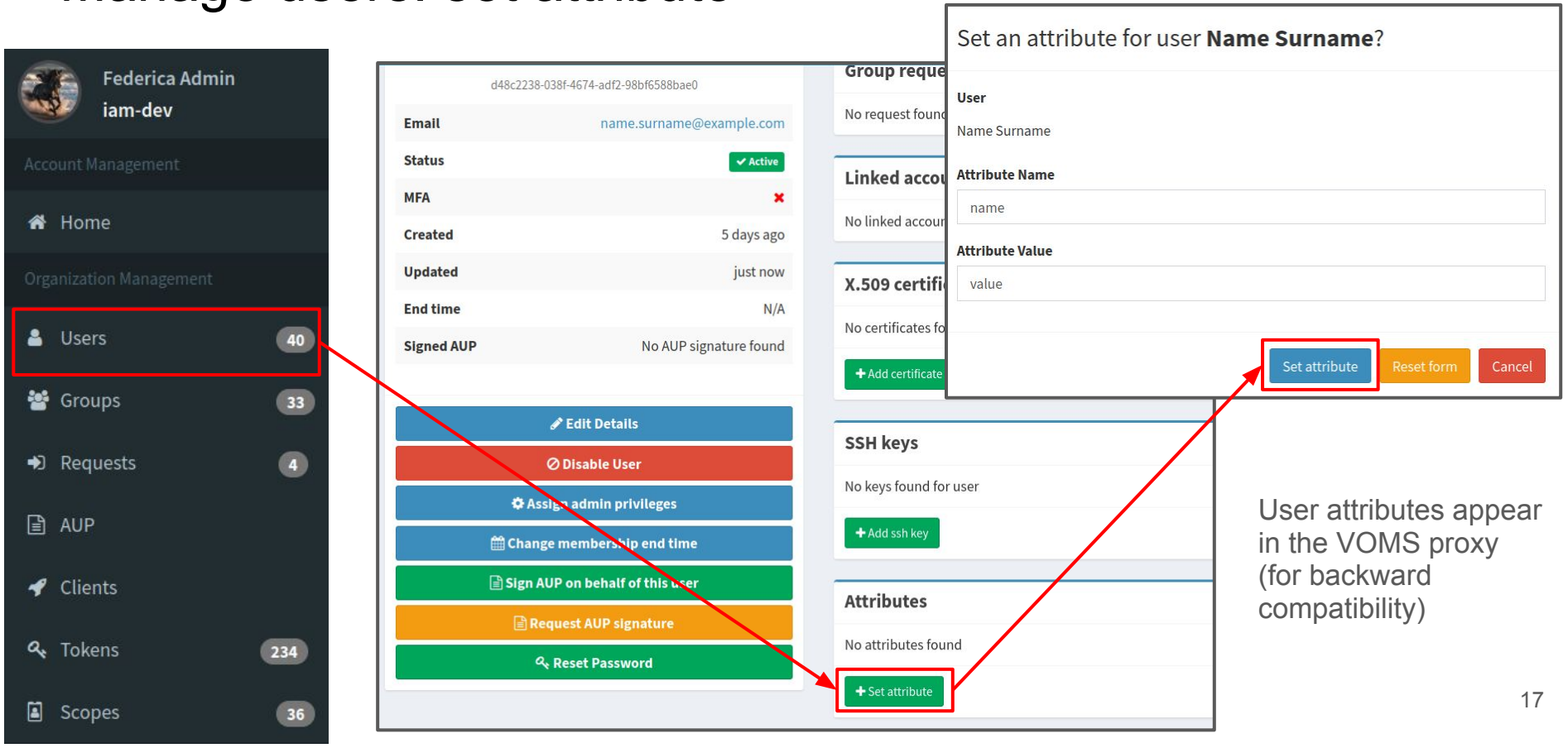
Manage users: add certificate



INDIGO IAM: a X.509 certificate can be added only in **PEM** format

VOMS Admin: it can be added in **PEM** format or by **Subject/Issuer DNs**

Manage users: set attribute



User attributes appear in the VOMS proxy (for backward compatibility)

Default attribute for newly created accounts

Upon request of WLCG, **INDIGO IAM** now allows to automatically add an attribute named *nickname* for newly created account (from IAM configuration), without requiring the user to set the proper attribute manually

This process happens both for login with external provider, or when one directly clicks on the *Apply for an account* button. The *nickname* value will be the same as the username set during the registration request

It is useful for services which identify the user through the attributes

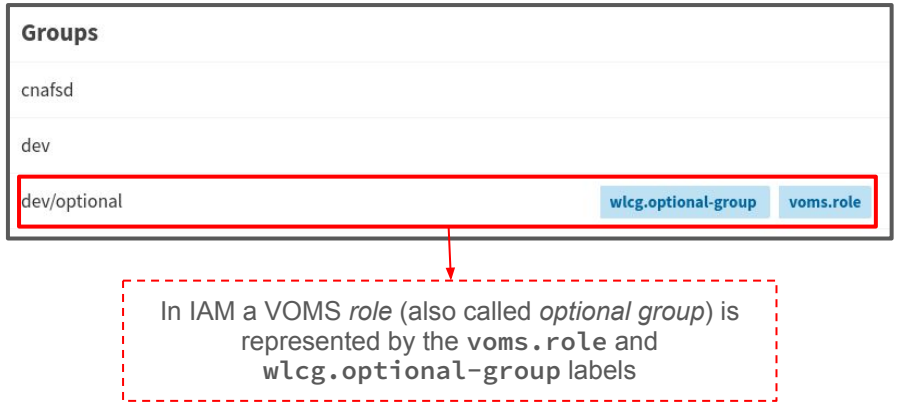
To enable this behavior (not present by default) one has to configure IAM as follows

```
iam:
  registration:
    add-nickname-as-attribute: true
```

Groups and roles

Both **INDIGO IAM** and **VOMS** support the concepts of *group* and *role*. As an example,

- group: **`/wlcg/xfer`** (VOMS) → **`wlcg/xfer`** (IAM)
- role: **`/wlcg/Role=test`** (VOMS) → **`wlcg/test`**, with labels (IAM)
- note the lack of a leading "/" in the IAM representation of groups



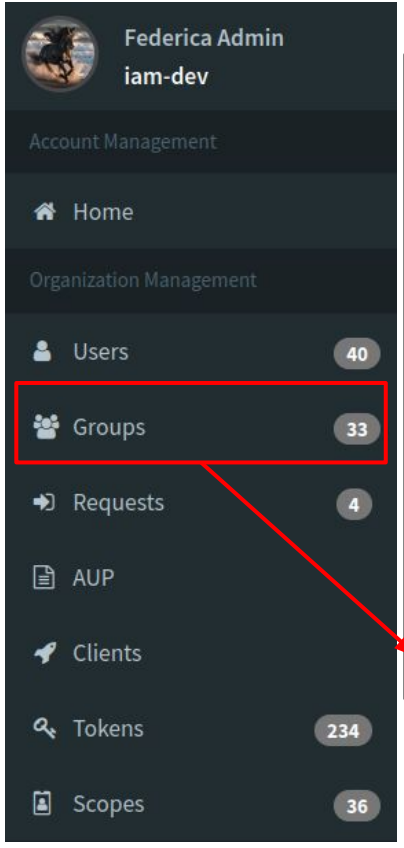
Roles

- **VOMS Admin**: they have to be explicitly requested (also multiple times)
- **INDIGO IAM**: the same behavior is obtained through *optional groups* for WLCG JWT tokens (the list of user's role memberships appears in the **`wlcg.groups`** claim)

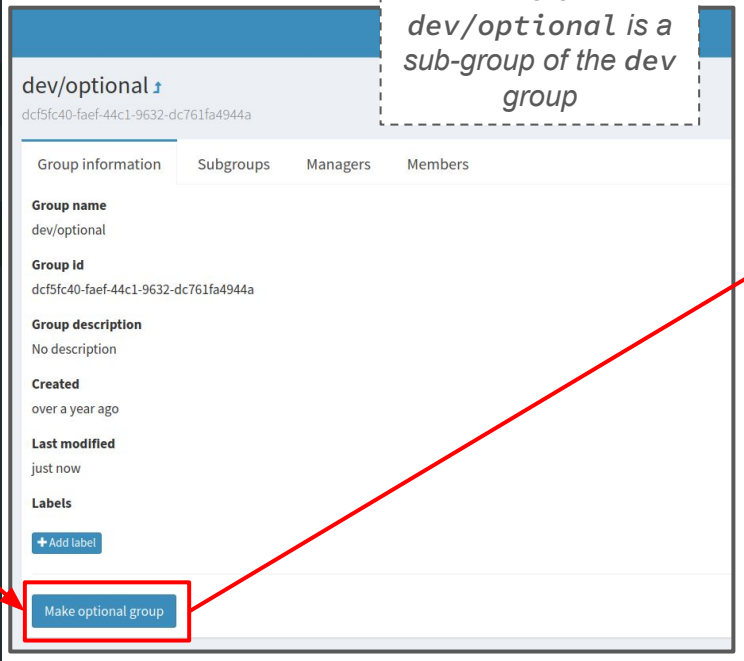
Primary groups

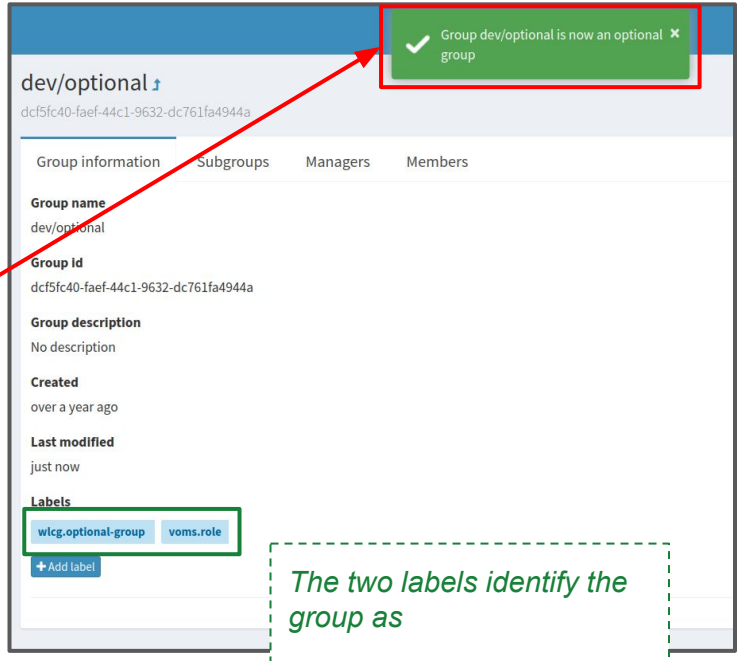
- **VOMS Admin:** the order of the requested group will be the same as the one appearing in the proxy
- **INDIGO IAM**: the same can be obtained for WLCG tokens while requesting **`wlcg.groups`** in a certain order

Manage groups: set a group as optional



Here `dev/optional` is a sub-group of the dev group

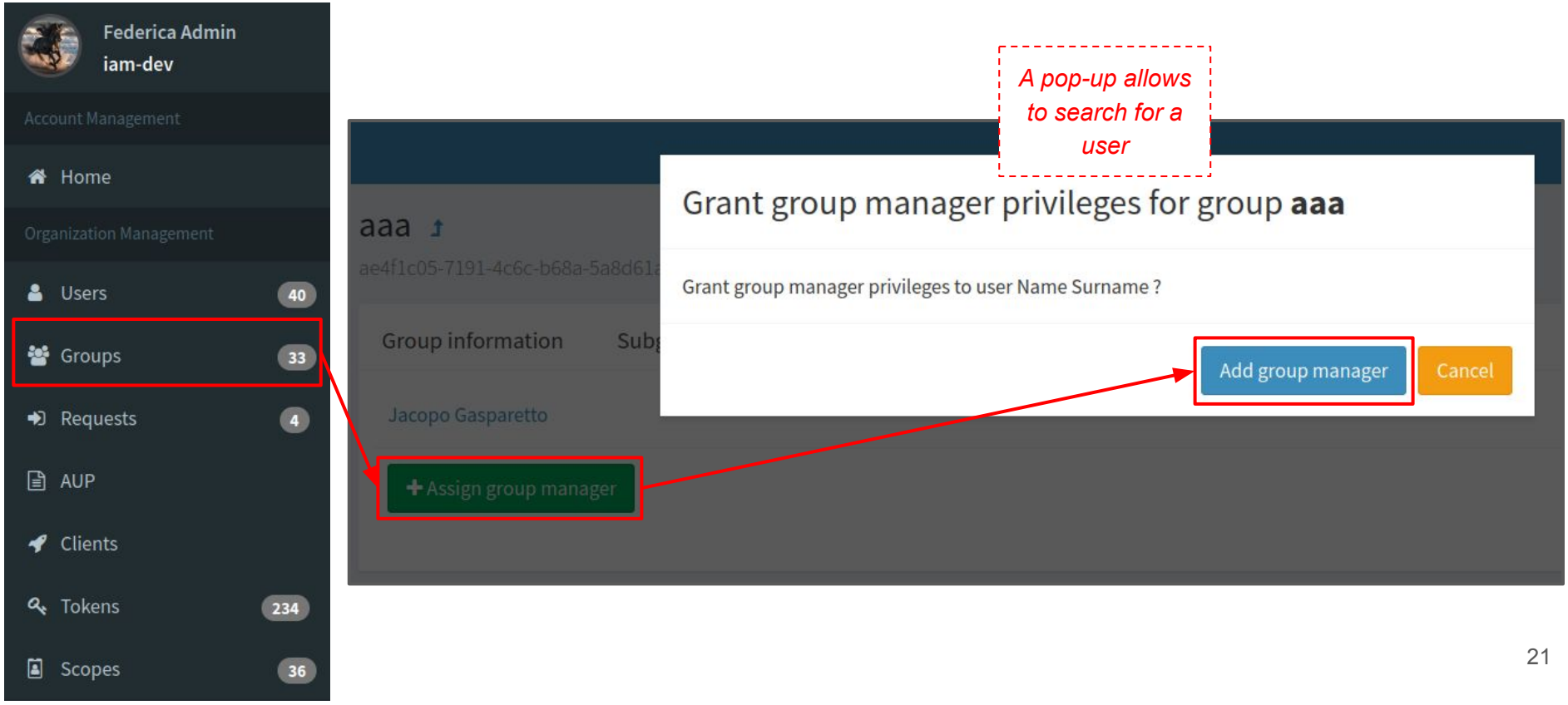




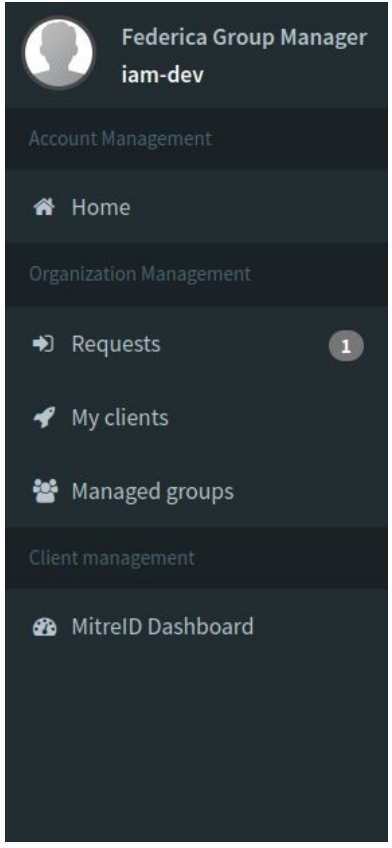
The two labels identify the group as

- *IAM optional group*
- *VOMS role*

Manage groups: assign group manager privileges



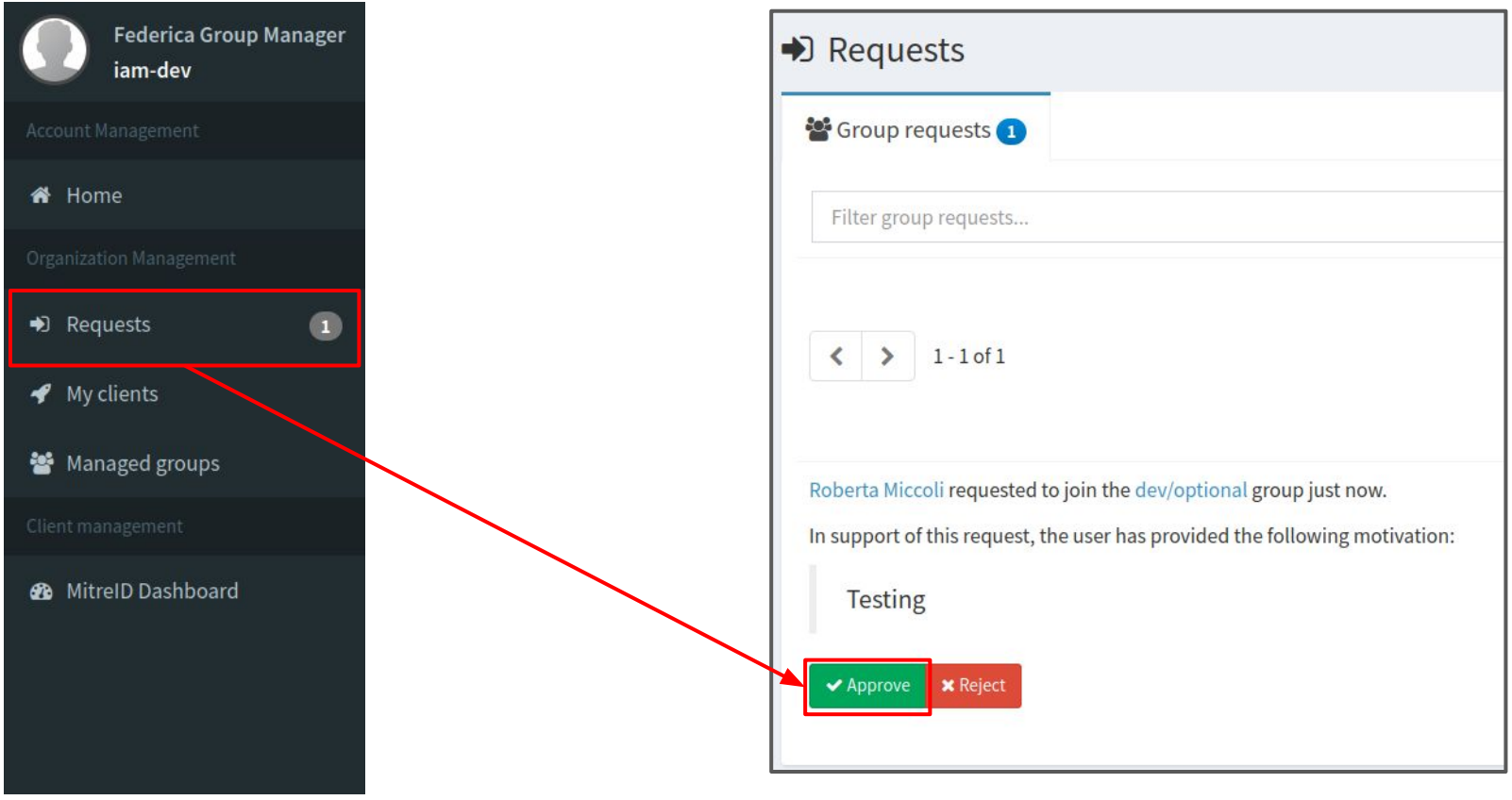
Group Managers



In **INDIGO IAM**, Group Managers (GM) can

- approve/reject group membership requests
- delete users from the managed groups
- view the list of sub-groups
- view the managers of the managed group
- view the list of group members
- *view some user information (to be fixed)*
    - *name, surname, uuid, username, email, status, created, updated, end time, labels*

Manage groups: requests



Default groups for newly created accounts

IAM allows to automatically add a newly created account to one or more group (from IAM configuration), without requiring a group enrollment phase

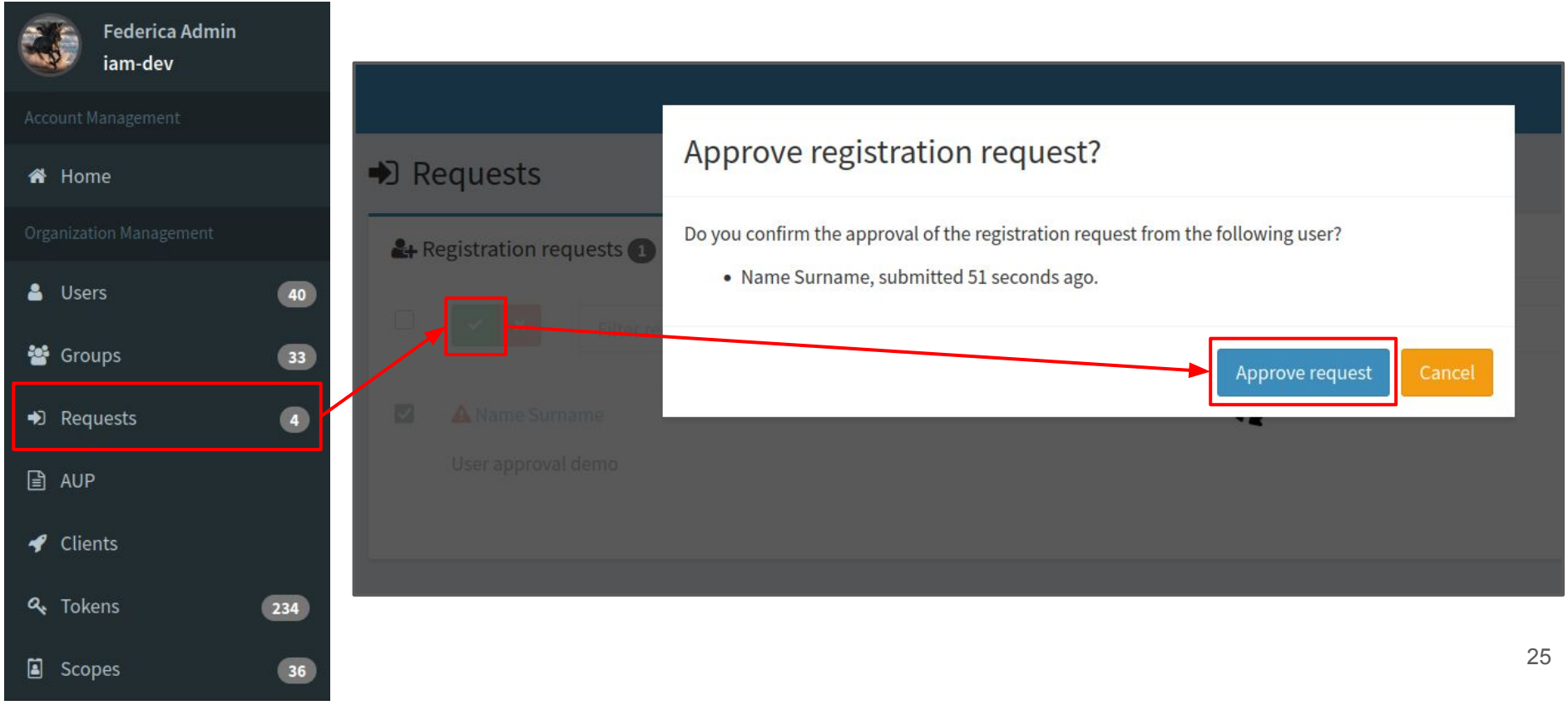
This is useful when we use VOMS-AA together with IAM, where in order to get a proxy the user must belong at leat to the root group equal to the VO name

For example, an Atlas VO may set the following configuration

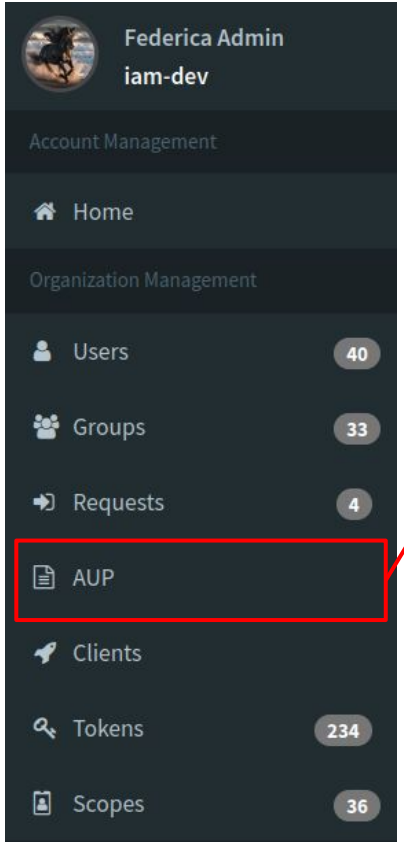
```
iam:
  registration:
    default-groups:
      - name: /atlas
        enrollment: INSERT
```

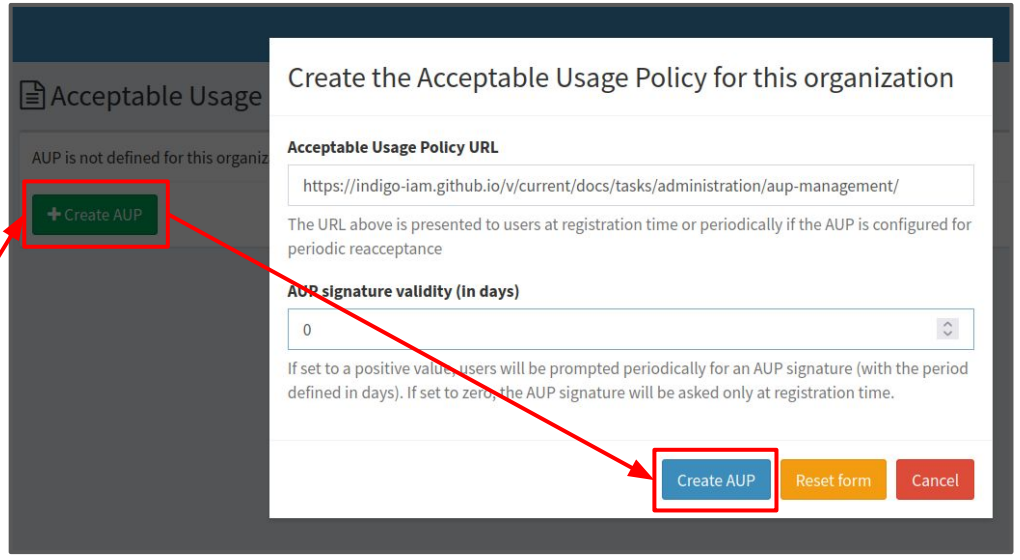
In the near future we will support an **`enrollment: GROUP_REQUEST`** property, which triggers a request to join the defined group, upon user registration. This is an hybrid mode, where a group request is sent to Admins/GM but the user does not have to request it manually

Approve VO membership requests



Set an AUP for a VO





An expired AUP signature forces the user to sign the AUP when the user tries to login into IAM and prevents the issuing of

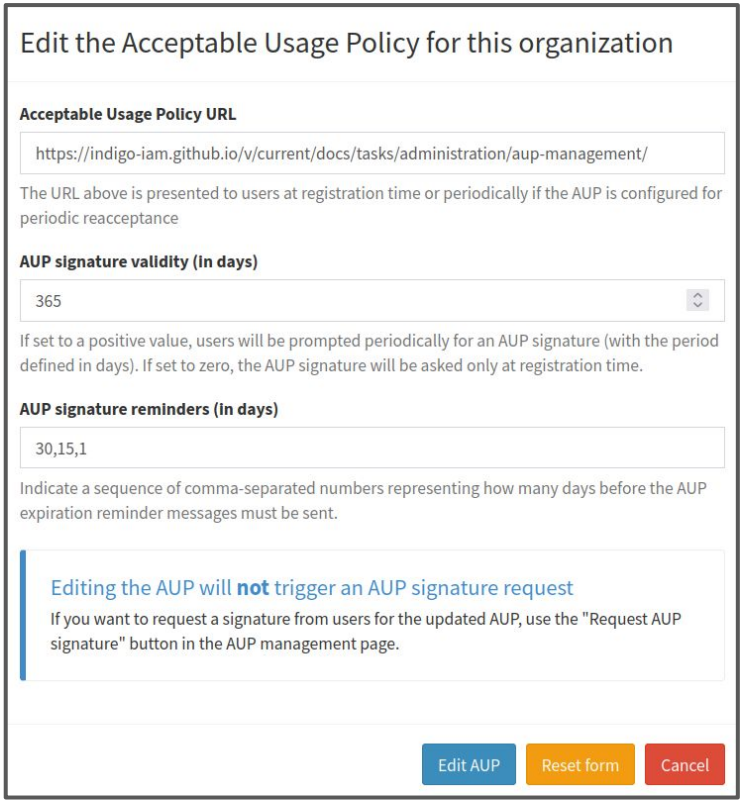
- access tokens
- VOMS proxies

Customize the AUP

VOMS Admin: the AUP is always present, to be signed by default every 365 days and a AUP reminder is sent before 30, 15 and 1 day from the expiration

INDIGO IAM: the AUP is highly customizable. By default it is not present, meaning no-one has to sign it, but an Admin can create one, and

- if the AUP validity is **set to 0**, the user is prompt to sign it just at registration time
- if it is a positive value, a new raw requesting **how many days before the AUP expiration**, a reminder message has to be sent



Some other features

Mail notification for account management

Admins perspective

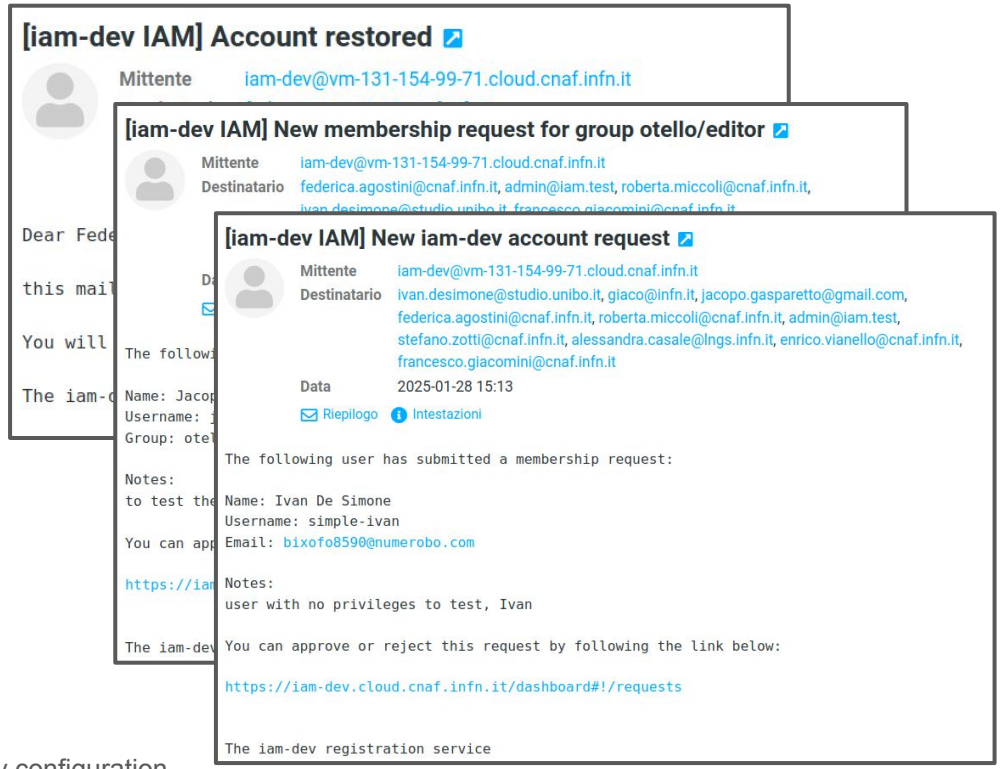
- Registration requests

Group managers and Admins perspective (*)

- Group membership requests

Users perspective

- Confirm/reject registration request
- Confirm/reject group request
- AUP reminders
- User suspension/restoration
- Password reset
- MFA enabled/disabled



(*) In IAM, the notification of group-related actions may be sent only to GM by configuration (`IAM_NOTIFICATION_GROUP_MANAGER_NOTIFICATION_POLICY=notify-gms`)

AUDIT logs

By default, the **INDIGO IAM** AUDIT logs are available to service operators in the IAM log (it differs from **VOMS Admin**, which exposes a web interface for auditing)

IAM AUDIT logs may be collected in a separate file by configuration

In INDIGO IAM, auditing operations include

- user's logging in/out
- add/remove user to a group
- add/remove user's label
- add/remove user's certificate
- access tokens, refresh tokens payload
- issuance of VOMS proxies
- etc.

Use this template to configure logs (e.g. log path and name) and copy it on IAM

Set the property
`logging.config=</path/to/log-config-file>`

AUDIT logs will be saved where indicated in your
`<log-config-file>`

They can be collected and made available (with an external service, e.g. OpenSearch) for instance to a group of privileged users

AUDIT logs example


```
2025-05-06T17:41:23.628+0200 INFO  7 --- [http-nio-8080-exec-6] AUDIT : {"@type":"ActiveReplacedEvent","timestamp":1746546083627,"category":"ACCOUNT","principal":"admin","message":"Replace user active status: false","account":{"uuid":"0a6fa72a-fb75-4a6c-9734-bfe673df70b3","name":"dup_email_1"},"updaterType":"ACCOUNT_REPLACE_ACTIVE","active":false,"source":"ScimUserProvisioning"}
2025-05-06T17:41:37.607+0200 INFO  7 --- [http-nio-8080-exec-6] AUDIT : {"@type":"IamAuthenticationSuccessEvent","timestamp":1746546097607,"category":"AUTHENTICATION","principal":"<unknown>","message":"test authenticated succesfully","sourceEvent":{"principal":"test","type":"AuthenticationSuccessEvent","details":{"remoteAddress":"172.18.0.1","sessionId":"701BDF2FC82CE7114662C4721189A696"}},"source":"ExtendedAuthenticationToken"}
2025-05-06T17:41:40.932+0200 INFO  7 --- [http-nio-8080-exec-1] AUDIT : {"@type":"RefreshTokenIssuedEvent","timestamp":1746546100928,"category":"TOKEN","principal":"client","message":"Issue refresh token","subject":"test","scopes":["openid","profile","offline_access","email"],"grantType":"authorization_code","payload":{"jti":"7e20816d-4ee8-4066-af11-9293c2706d99"},"source":"IamTokenService"}
2025-05-06T17:41:41.013+0200 INFO  7 --- [http-nio-8080-exec-1] AUDIT : {"@type":"AccessTokenIssuedEvent","timestamp":1746546101010,"category":"TOKEN","principal":"client","message":"Issue access token","scopes":["openid","profile","offline_access","email"],"subject":"test","grantType":"authorization_code","header":{"kid":"rsa1","alg":"RS256"},"payload":{"iss":"https://iam.test.example/","iat":1746546100941,"exp":1746549700902,"sub":"80e5fb8d-b7c8-451a-89ba-346ae278a66f","jti":"adae0623-776a-4c12-9ada-304fbc37d20b","client_id":"client","nbf":1746546100941,"scope":"openid profile offline_access email","wlcg.ver":"1.0","aud":["https://wlcg.cern.ch/jwt/v1/any"]},"refreshTokenJti":"7e20816d-4ee8-4066-af11-9293c2706d99","source":"IamTokenService"}
2025-05-06T17:41:41.287+0200 INFO  7 --- [http-nio-8080-exec-8] AUDIT : {"@type":"IamAuthenticationSuccessEvent","timestamp":1746546101287,"category":"AUTHENTICATION","principal":"<unknown>","message":"client authenticated succesfully","sourceEvent":{"principal":"client","type":"AuthenticationSuccessEvent","details":{"remoteAddress":"172.18.0.2","sessionId":null}},"source":"UsernamePasswordAuthenticationToken"}
2025-05-06T17:41:50.757+0200 INFO  7 --- [http-nio-8080-exec-4] AUDIT : {"@type":"IamAuthenticationSuccessEvent","timestamp":1746546110757,"category":"AUTHENTICATION","principal":"<unknown>","message":"admin authenticated succesfully","sourceEvent":{"principal":"admin","type":"AuthenticationSuccessEvent","details":{"remoteAddress":"172.18.0.1","sessionId":"EAE24FA7AB2007EA0073BE6FE0F4D776"}},"source":"ExtendedAuthenticationToken"}
2025-05-06T17:42:10.427+0200 INFO  7 --- [http-nio-8080-exec-9] AUDIT : {"@type":"UsernameReplacedEvent","timestamp":1746546130426,"category":"ACCOUNT","principal":"admin","message":"Replace user username: mfa","account":{"uuid":"467c882e-90da-11ec-b909-0242ac120002","name":"mfa"},"updaterType":"ACCOUNT_REPLACE_USERNAME","username":"mfa","source":"ScimUserProvisioning"}
2025-05-06T17:42:21.614+0200 INFO  7 --- [http-nio-8080-exec-2] AUDIT : {"@type":"AupCreatedEvent","timestamp":1746546141612,"category":"AUP","principal":"admin","message":"AUP created","aup":{"id":null,"name":"default-aup","description":null,"signatureValidityInDays":0,"aupRemindersInDays":"","creationTime":1746546141599,"lastUpdateTime":1746546141599,"url":"http://example.org","text":null},"source":"DefaultAupService"}
2025-05-06T17:42:28.779+0200 INFO  7 --- [http-nio-8080-exec-9] AUDIT : {"@type":"IamAuthenticationSuccessEvent","timestamp":1746546148779,"category":"AUTHENTICATION","principal":"<unknown>","message":"admin authenticated succesfully","sourceEvent":{"principal":"admin","type":"AuthenticationSuccessEvent","details":{"remoteAddress":"172.18.0.1","sessionId":"5375CC52588926E1390A2148F9B1869E"}},"source":"ExtendedAuthenticationToken"}
2025-05-06T17:42:30.111+0200 INFO  7 --- [http-nio-8080-exec-5] AUDIT : {"@type":"AupSignedEvent","timestamp":1746546150110,"category":"AUP","principal":"admin","message":"User admin signed the AUP","signature":{"aupId":1,"username":"admin","signatureTime":"2025-05-06T17:42:30.092+02:00"},"source":"AupSignaturePageController"}
```

Multiple authentication mechanisms

INDIGO IAM supports multiple authentication mechanisms

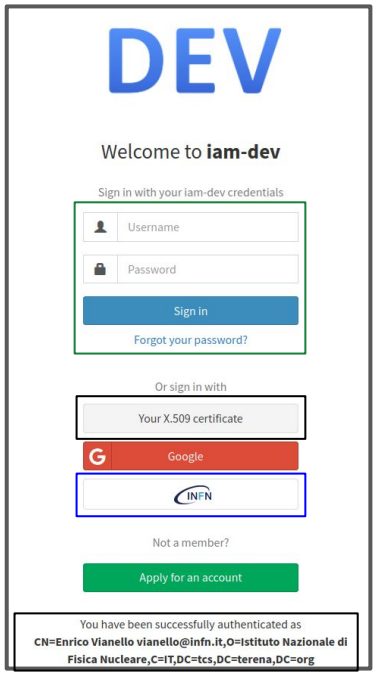
- username/password
- X.509 certificates
- OIDC providers (CERN SSO, Google, etc.)
- SAML Identity providers (e.g. INFN)
- SAML federations (e.g. EduGAIN)
- (near future:) OIDC Federations

Local credentials may be disabled by IAM configuration

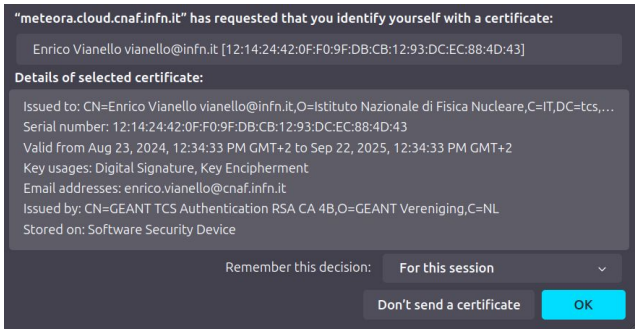
The *X.509 certificate* button appears just if one selects the certificate imported in the browser when it pops up (as in VOMS)

The *Apply for an account* button may be hidden if users are forced to login through trusted external providers

Login to INDIGO IAM



Login to VOMS Admin server



The **VOMS Admin** authentication involves just X.509 certificates

Customization of the VO dashboard

VOMS Admin embeds a dashboard for Admin and users

Efforts have been made in **INDIGO IAM** to decouple front-end from back-end

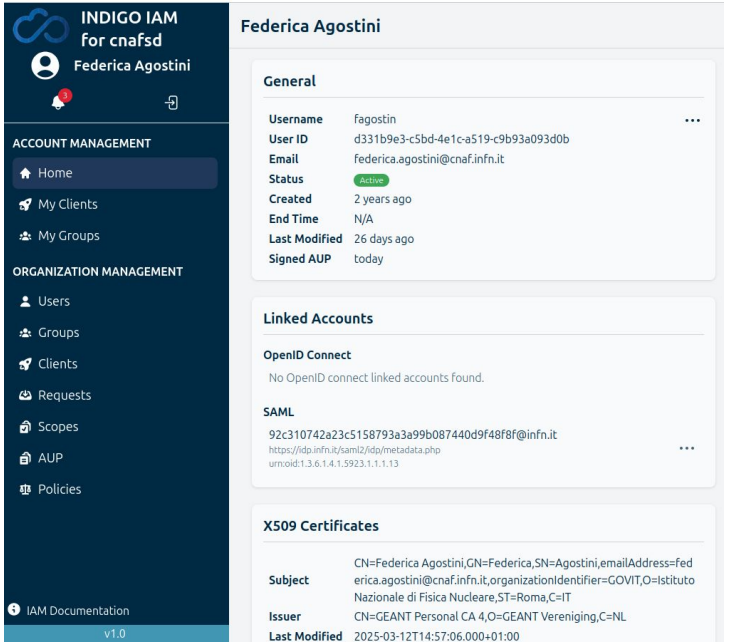
- INDIGO IAM APIs expose many information
- access to APIs is also moderated by admin/user token **scopes**

It allowed to develop a new INDIGO IAM dashboard

- driven by the current dashboard based on **JavaServer Pages** (JSP) and **Angular.js**, in EOL since January 2022
- new dashboard is based on Next.js web framework
- components are written in React
- implements a Backend for Frontend (BFF) pattern

Any community may develop its own dashboard

User's page of the INDIGO IAM React-based dashboard



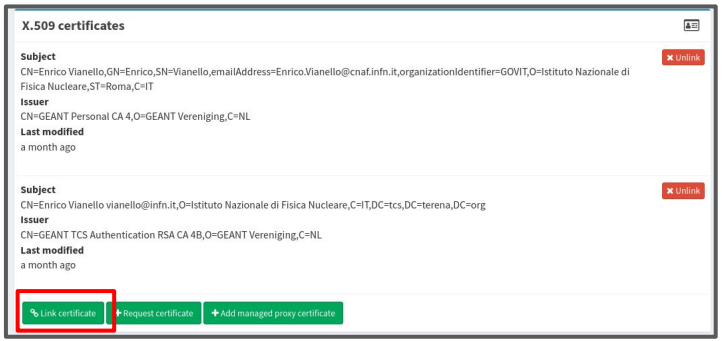
https://iam-dashboard.cloud.cnaf.infn.it/

Self service upload of user DN

In **VOMS Admin**, an X.509 certificate can be linked to an account as **PEM** format or by **Subject/Issuer DNs**. This may happen for both an Admin perspective (adding a certificate to a user), or a user perspective

INDIGO IAM allows uploading an X.509 certificate as follows

- user perspective
  - link the certificate at login phase when requested by the browser
  - login to IAM
  - add the certificate through the *Link Certificate* button
  - no way to self-upload a certificate via PEM format, or Subject/Issuer DNs



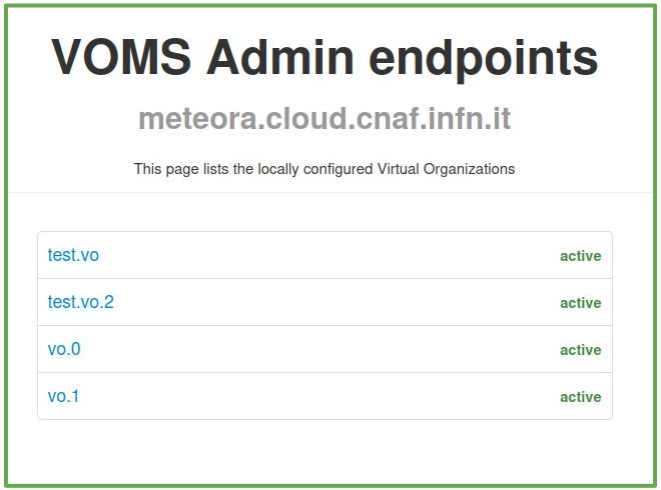
- Admin perspective: copy-and-paste the certificate in **PEM** format

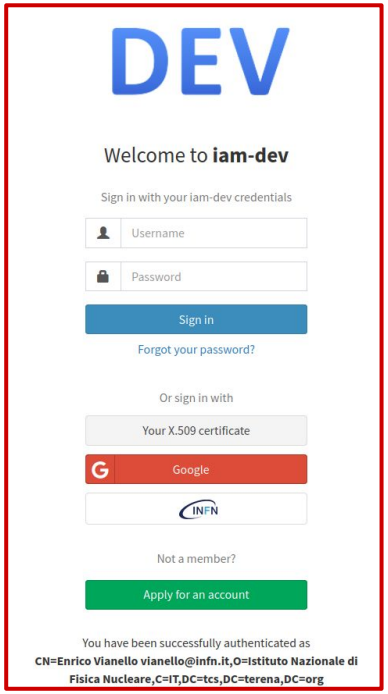
The self-service upload of user certificate was included in PR #750, but reverted since a security discussion is still ongoing (issue #527)

Multi VO

VOMS Admin supports the concept of multi-VO

INDIGO IAM only serves 1 VO per IAM instance





There are discussions (#711 plus some issues) on how to make IAM multi-VOs

For now, some communities (e.g. ESCAPE) use the IAM groups to identify different VO/experiments

This could work with tokens somehow, but not for proxies, where the parent group MUST be equal to the VO name

- unless adding one VOMSAA per parent group

For tokens, the issuer will be the same for different groups/VOs

Hands-on

Hands-on

The previous examples have been performed with https://iam-dev.cloud.cnaf.infn.it

Anyway, to access to the Admin interface a self-contained deployment with docker-compose is available here

If you like, fork it and customize your IAM instance

To play with the Admin interface, you can use the already populated IAM db where, among others, you can find the following 2 users

- Admin user, with credentials *admin/password*
  - create a Group Manager user
- normal user, with credentials *test/password*