eduroam Managed IdP (Pilot)

Product Description and Implementation Status

The product outsources the technical setup of eduroam IdP functions to the eduroam Operations Team. The system includes

- a web-based user management interface where user accounts and access credentials can be created and revoked (there is a limit to the number of active users)
- a technical infrastructure ("CA") which issues and revokes credentials
- a technical infrastructure ("RADIUS") which verifies access credentials and subsequently grants access to eduroam
- TBD: a lookup/notification system which informs you of network abuse complaints by eduroam Service Providers that pertain to your users

See also this 

for more infos about the product!

Policy / User Account Liability

As an eduroam IdP administrator using this system, you are authorized to create user accounts according to your local institution policy. You are fully responsible for the accounts you issue. In particular, you

- only issue accounts to members of your institution, as defined by your local policy.
- must make sure that all accounts that you issue can be linked by you to actual human end users of eduroam
- have to immediately revoke accounts of users when they leave or otherwise stop being a member of your institution
- will act upon notifications about possible network abuse by your users and will appropriately sanction them

Failure to comply with these requirements may lead to the deletion of your IdP (and all the users you create inside) in this system.

Privacy

With this product, we are not interested in and strive not to collect any personally identifiable information about the end users you create. To that end,

- the usernames you create in the system are not expected to be human-readable identifiers of actual humans. We encourage you to create usernames like 'hr-user-12' rather than 'Jane Doe, Human Resources Department'. You are the only one who needs to be able to make a link to the human behind the identifiers you create.

- the identifiers in the credentials we create are not linked to the usernames you add to the system; they are pseudonyms.
- each access credential carries a different pseudonym, even if it pertains to the same username.
- to allow eduroam Service Providers to recognise that the same user is using their hotspot (even if using multiple devices and thus different pseudonyms), TBD: we send a RADIUS attribute to allow this grouping ('Chargeable-User-Identity'). That value is sent only on request of the Service Provider, and different Service Providers get different values; even for the same access credential of the same user.

Internal SLAs

- The pilot is run on a best-effort basis.
- Uptime of the VMs running the service is undefined (GEANT development VMs running on the Greek 'Okeanos' platform, no high availability). Aiming at 99% plus is probably an understatement, but not commited.
- First reaction to bugs (triage, checking reproducability) is targeted for three business days after reporting. **Please report bugs/feature requests via GitHub.**

Pilot Phase Location, Feature Activation

The pilot is accessible via the web page https://cat-pilot.eduroam.org. That web page contains recent development snapshot which is considered usable enough to allow pilot testing. It may be updated throughout the pilot runtime for bug fixing, feature additions or UI changes as found during the pilot test.

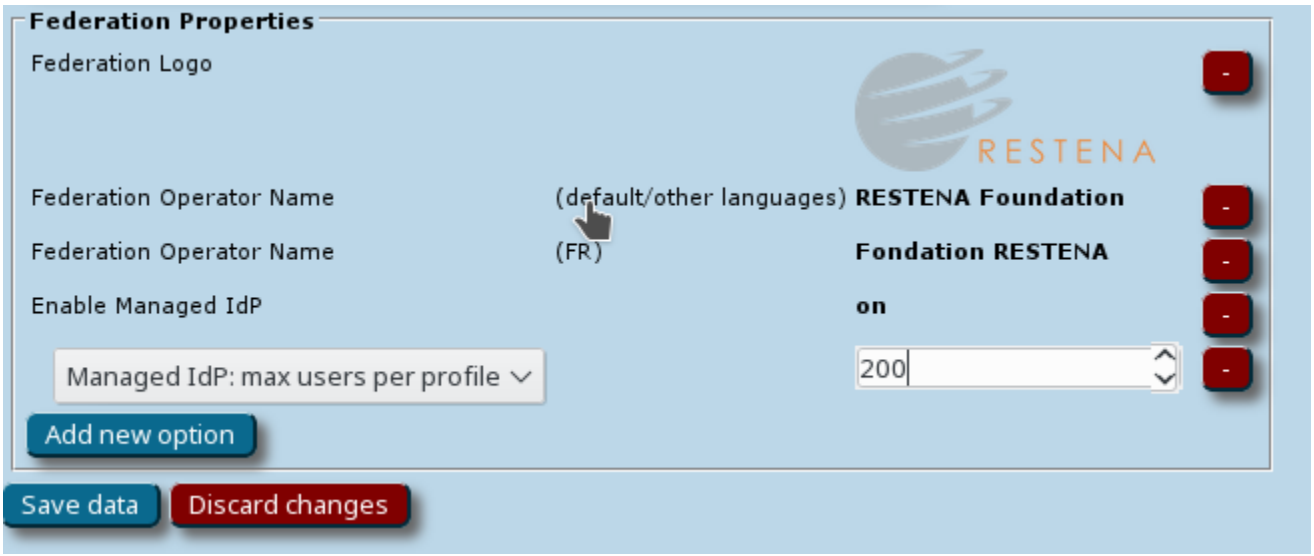
The test site is connected to the usual eduroam Operations Support Systems and access is managed in the same way as in eduroam CAT proper: if you have NRO level access to eduroam CAT and log in with the same credential, you will also have NRO level access on the test site.

The test site starts with an empty institution database. As an NRO admin, you invite participants as you usually do. Note that it is in principle possible to also test other features of the upcoming eduroam CAT 1.2 on this site, but this is not the focus and the developers do not assert that any of the other features function as designed. The focus of this deployment is exclusively eduroam Managed IdP.

Federation Administrator: enable and configure Managed IdP

With a click on the usual "Click here to manage your federations" you can now see that your federation has federation-level properties (which it did not have in CAT 1.1):

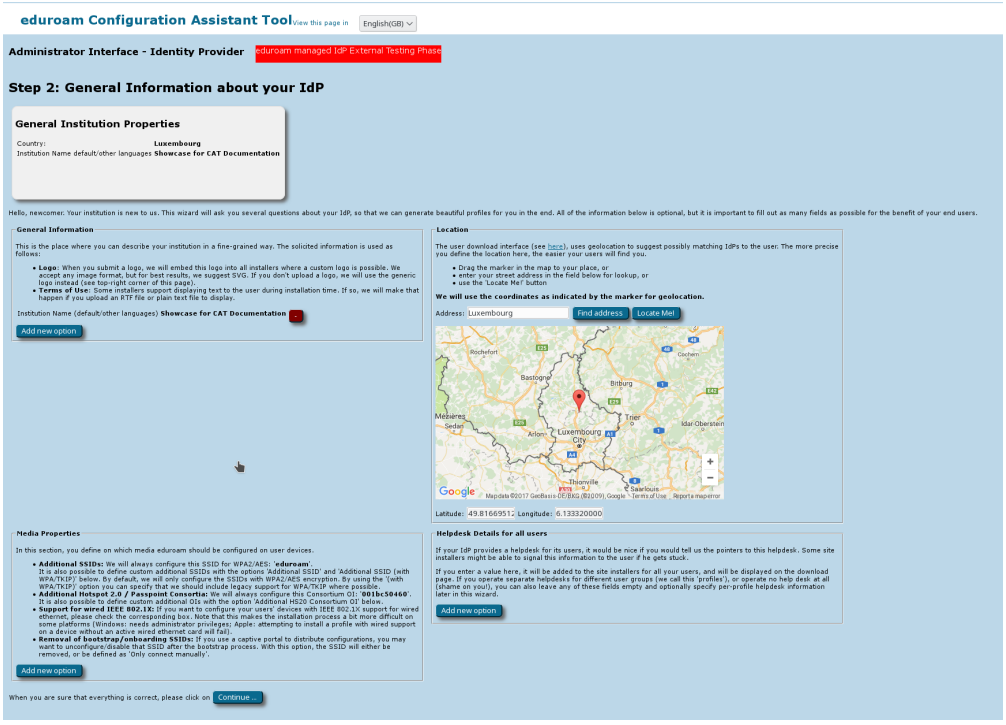
With a click on "Edit", you can enable the feature. The default maximum number of users an IdP can manage in the system is 200; if you want to set a different maximum, you can do that by also setting the "max users per profile" option. The third option, "Do not terminate EAP" does not currently have any function.



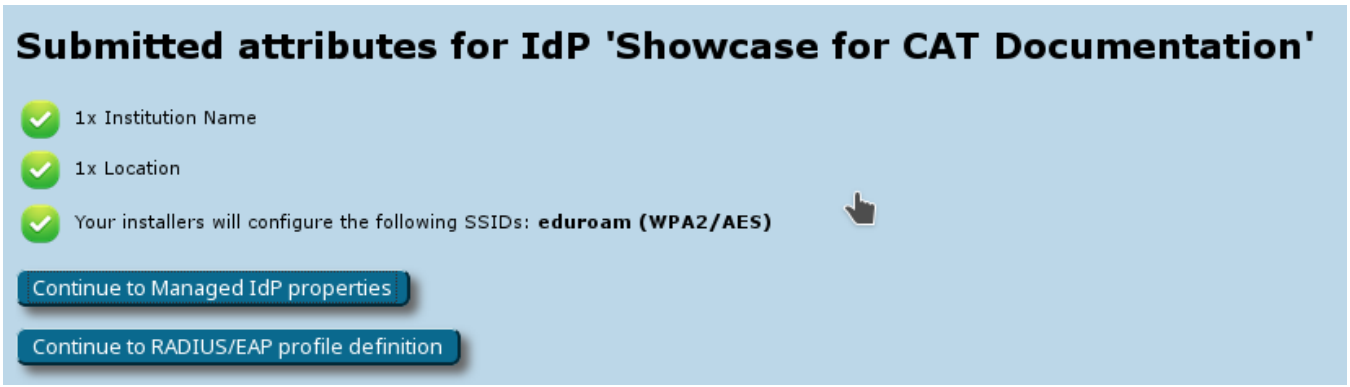
IdP Administrator: enrollment

The initial IdP signup remains unchanged compared to CAT 1.1: federation operators send email invitations to new admins as usual; there is no distinction between future "RADIUS" IdPs vs. "Managed" IdPs. Administrators log in with either their eduGAIN credential or a social network account as described in the main CAT manual.

The choice whether to become a RADIUS vs Managed IdP is with the IdP administrator. Please report any issues with that choice as part of the pilot usage reporting. For reference, a new IdP typically gets presented the following page, where any number of additional institution properties can be added (with 'Add new option'); all of those options can be left unchanged if the administrator so wants.

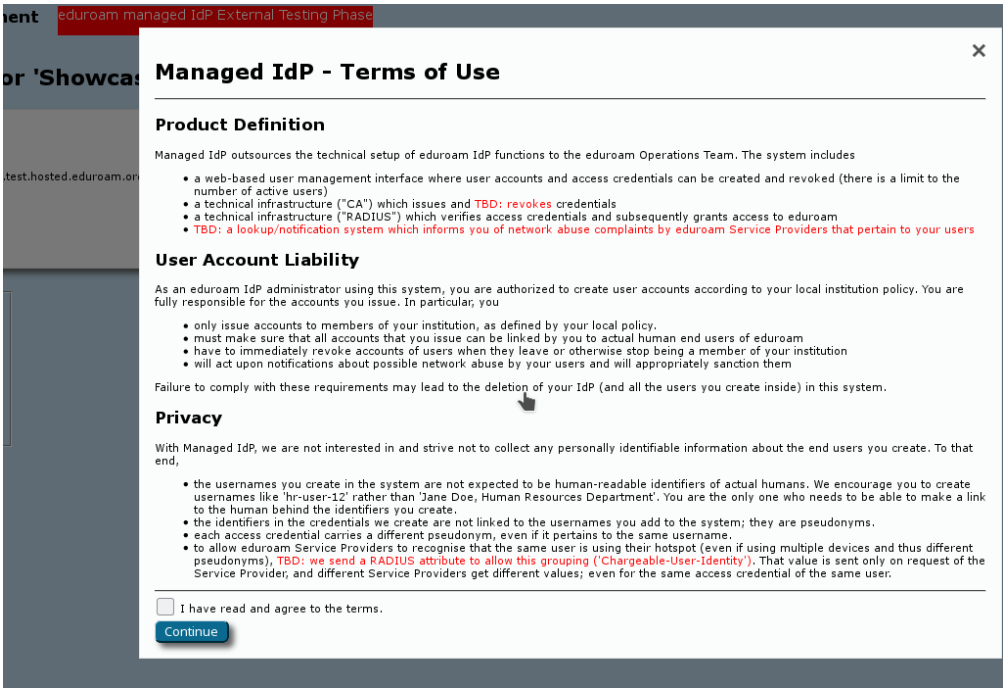


After a new IdP administrator logs into CAT, during the institution setup wizard, and only when the product is enabled by the respective federation administrator, there is a new choice to make after making the institution-wide settings:



This is an EXCLUSIVE choice: once a RADIUS/EAP profile has been chosen, Managed IdP becomes unaccessible. And if a Managed IdP profile gets chosen, RADIUS/EAP cannot be configured any more. It was a product design decision not to allow both. Please report any issues with that choice as part of the pilot usage reporting.

For the purposes of this pilot, it is of course expected that administrators choose the Managed IdP option. After doing so, the IdP admin is presented with the Terms of Use screen. The product can only be used after the Terms of Use have been accepted:



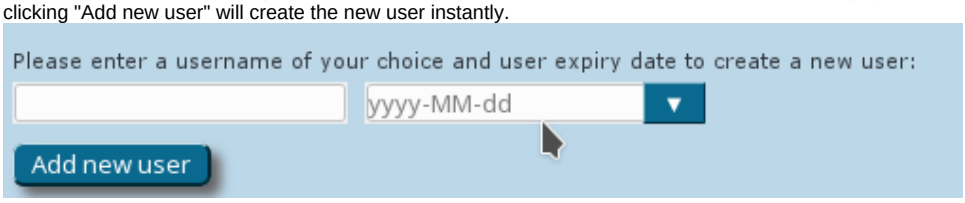
IdP administrator: usage

There is only one screen from which new user accounts can be created or imported, credentials can be assigned, and existing credentials and users can be decommissioned.

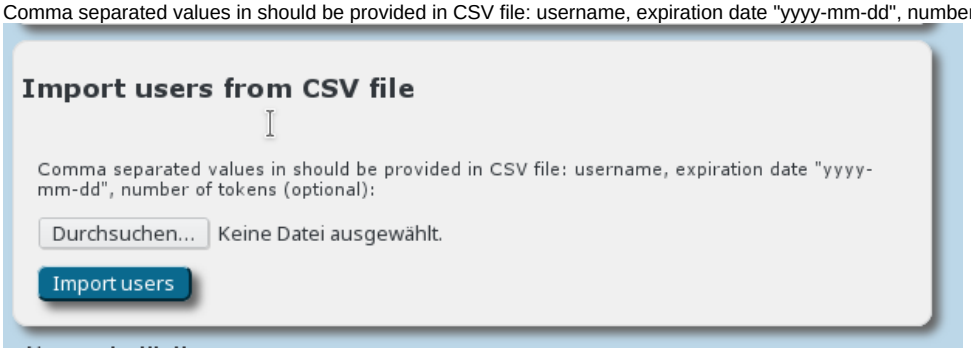
Adding Users

There are two workflows for adding new users:

- Manual: on the bottom of the page, there is an input box for a new username and the desired expiry date for that user. Filling in both and then clicking "Add new user" will create the new user instantly.



- CSV import: for a bulk import of many users, there is a grey box: "Import users from CSV file" near the top of the page. The format of the CSV file is:
  Comma separated values in should be provided in CSV file: username, expiration date "yyyy-mm-dd", number of tokens (optional):

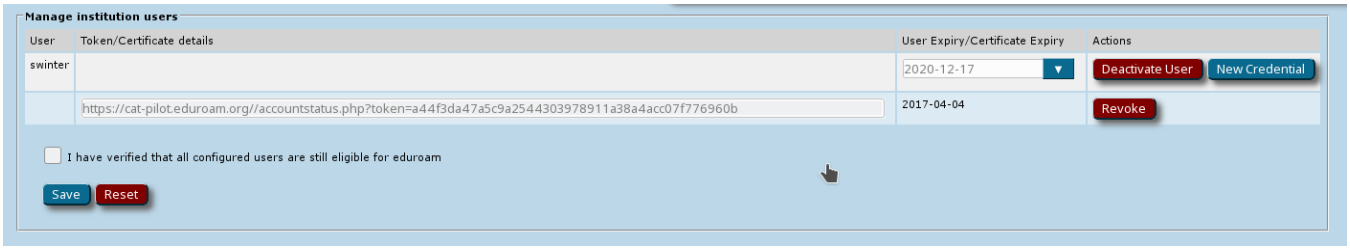


It is part of the pilot evaluation whether these two choices for adding users are sufficient, or if other means should be added. Please ask your pilot participants about their preference here.

Issuing access credentials

Once a user is created, it is displayed on the page along with Delete and New Credential buttons. Clicking on "New Credential" creates an invitation URL. The URL is then displayed on the administration page. It is up to the administrator how to get that URL to the user in question. We expect this to happen usually over email, but it is part of the pilot phase evaluation whether leaving the means up to the admin (as implemented now) is a good way forward; alternatives include allowing to send an email directly from the interface, allowing text messaging, send via popular messengers, etc.

Invitation links are valid for one week from issuance, for the generation of a single access credential. The validity for the pickup by the end user is displayed to the right of the invitation link. Invitation links can be revoked by clicking the corresponding button on the right.

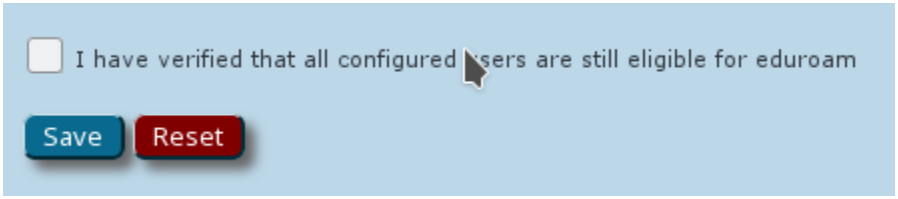


Credential revocation and Deadman Switch

Once a credential has been picked up by the end user, the corresponding certificate details are displayed instead of the invitation link. The "Revoke" button, if pushed, then revokes the already issued access credential and makes the login with it unusable. We strive towards a delay of less than one minute between push of the Revoke button and actual discontinuation of service for the end user.

When a user gets deleted, all his credentials automatically get revoked instantly.

WARNING: there is a "deadman switch" safeguard against unmaintained accounts. An IdP administrator may forget about his duties to maintain a current and accurate user list in the system, or the IdP administrator may leave the organisation with noone realising that stale accounts are still active. The safeguard is: the IdP admin must log into the system regularly and declare that he is still active and that all users which are currently active in the system continue to be eligible for eduroam. Failure to acknowledge this with the push of the corresponding button deletes all users and thus revokes all access credentials.

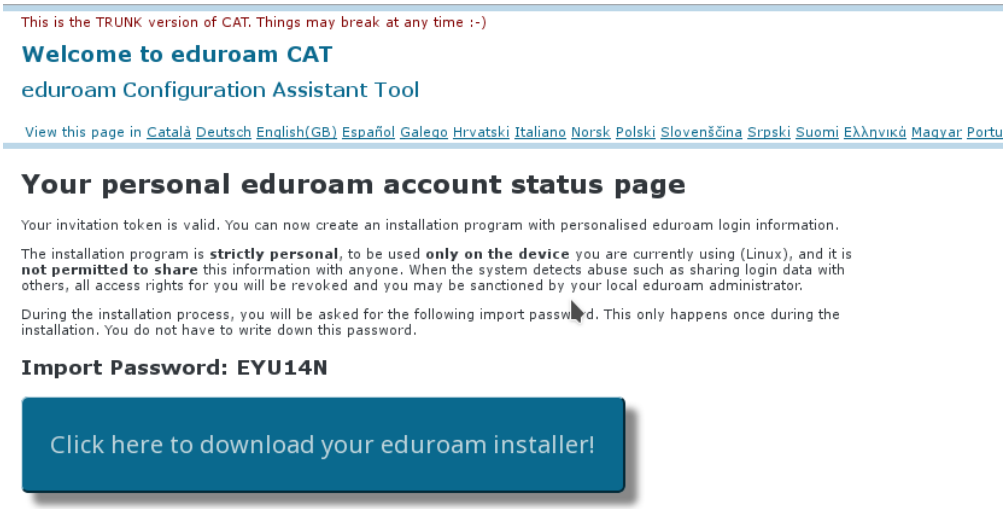


The system currently requires the re-validation once per year. Users which were not re-validated within the last 47 weeks are shown in yellow; users which were not re-validated within the last 50 weeks are displayed in red.

End-User

Enrollment

The interface to end users is as lightweight as possible. Upon visiting the invitation link, there is only a single download button along with basic instructions. The operating system is auto-detected and cannot be changed. Please report in the pilot evaluation whether this worked sufficiently well for your users.



The installation program is a CAT installer like usual, with the addition of a client certificate which is protected by the import password that is displayed on the screen. The addition of the import password provides a basic safeguard against credential sharing. Other safeguards (which could replace this UI-intensive step) such as maximum amount of MAC addresses are under consideration. Please report how well the import password method works for your users.

Ongoing status

Once the eduroam credential is issued, the invitation link turns into an access link to the current status of all access credentials of the user. The user can review the expiry date, whether a credential was revoked, which devices any of his invitation links was bound to, and the certificate details with which his

eduroam login is done

TBD: Access to status page without token value should still work with the client certificate. Not implemented yet.

eduroam usage

The installer sets up everything. The user should not need to interact with his operating system at all (at least, not any more than with other eduroam accounts).

One invitation, one credential

There have been extensive discussions how best to implement the invitation and enrollment system for end users. The current implementation binds exactly one invitation link to exactly one eduroam access credential on one device. As a consequence, users who want to configure eduroam on more than one device need to request several invitiation links (or manually go through complex processes to export and import client certificates and eduroam configurations; our working assumption is that end users can't usually be bothered to do this).

Alternatives were considered, and we would like to hear from you in the pilot evaluation whether these, or any other additional alternatives you can think of are possibly a better approach:

- Unlimited credentials during the one-week validity period of the invitation link: enables multi-device enrollment. Makes harder to detect "MITM" stealing of the invitation link & makes account sharing easier by sharing the one golden link with all your friends.
- fixed number of credentials during the one-week validity period (say, 3?): enables multi-device enrollment, without easy sharing of account. More difficult to communicate to end user when validity ends.