A guide to eduroam CAT for federation administrators

eduroam CAT: Purpose and scope

eduroam CAT is the *eduroam Configuration Assistant Tool*. Its purpose is to allow authorised eduroam Identity Providers to generate customised eduroam installers for various platforms, and to debug their RADIUS setup. Authorisation for IdPs to use eduroam CAT is determined by the eduroam National Roaming Operator (the eduroam "federation").

eduroam is organised in national federations. A federation administrator works at the eduroam National Roaming Operator (NRO) and accredits new eduroam IdPs, changes IdP details, or deprovisions eduroam IdPs. The primary vehicle for this is not eduroam CAT, but the official eduroam database, which contains all registered IdPs and their contact details.

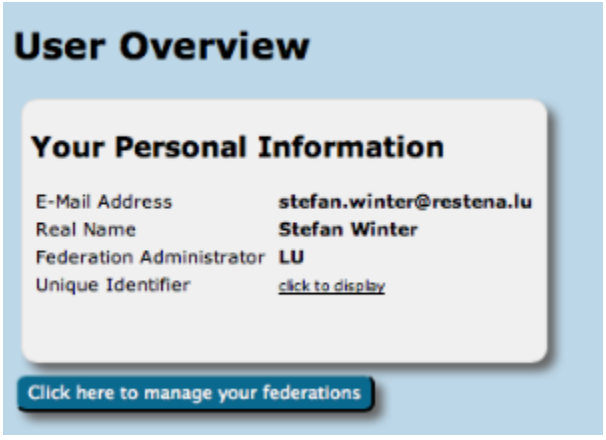
An eduroam federation administrator can invite his IdPs to make use of the eduroam CAT if he wishes to; enabling or disabling IdPs for eduroam CAT is done inside the eduroam CAT administration interface. This interface does not replace an NROs internal customer relationship management system; in particular, CAT does not export data into the official eduroam database; it only consumes data from that database. An NRO is still required to maintain records of all its IdPs and SPs on its own, and to export the corresponding data to the official eduroam database.

Managing my federation

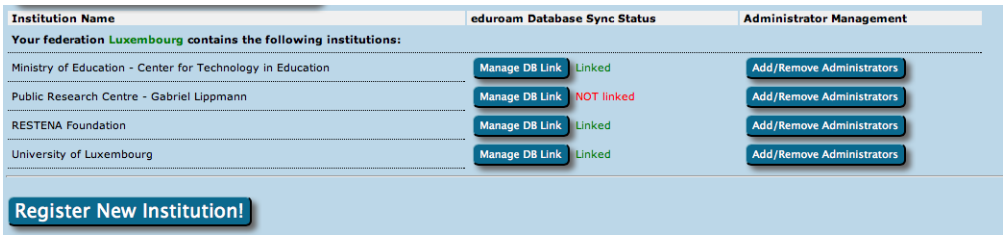
For users with the federation management privilege, eduroam CAT provides a dedicated web interface which allows federation administrators to

- invite a new IdP to use eduroam CAT
- add new representatives to existing IdPs
- delete representatives of existing IdPs
- take control over an IdP
- manage the relationship between an IdP in eduroam CAT vs. an IdP in the official eduroam database

All of these functions are accessible after logging into eduroam CAT with an account with the federation operator privilege. With such a user account, a new button will be displayed in the personal overview page: "Click here to manage your federations". NB: if you are a federation administrator, but do not have a privileged account yet, please see the guide to eduroam Operations Support Services for federation administrators (here).



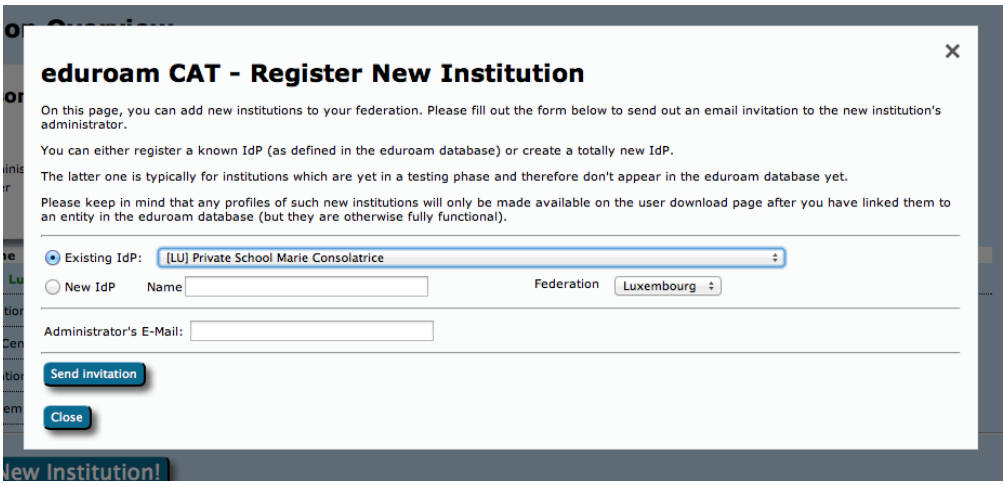
After clicking the button, an overview of the federation occurs, with entry points for the tasks mentioned above.



Invite a new IdP to use eduroam CAT

The button on the lower end of the page allows you to send an invitation to use eduroam CAT to an IdP in your federation. This can either be an IdP which is already in production (i.e. already listed in the official eduroam database with at least the "IdP" role) or it can be a new institution which is still in a bootstrapping phase (i.e. not yet registered in the official eduroam database).

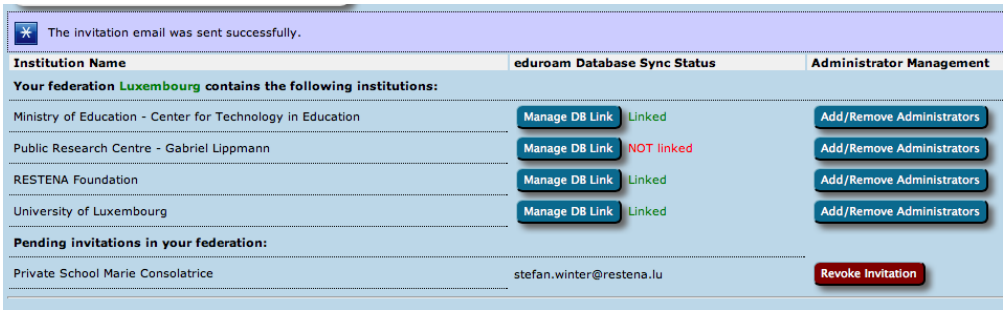
After clicking the button, the following window will appear, which allows to take the required actions:



You can either select an institution which is already listed in the eduroam database ("Existing IdP") or you can instead use the "New IdP" row to enter an institution name and federation by hand.

In both cases, you need to enter the email address to send the invitation to. Before actually sending the invitation, keep in mind that the invitation token for the IdP admin will only be valid for 24h; and that the token can only be consumed once. It is thus wise to check that the mail address is going to be read in the next business day; and that tokens sent to a mailing list will only be valid for the first person who redeems the invitation token. It may be a good idea to use personal email addresses only.

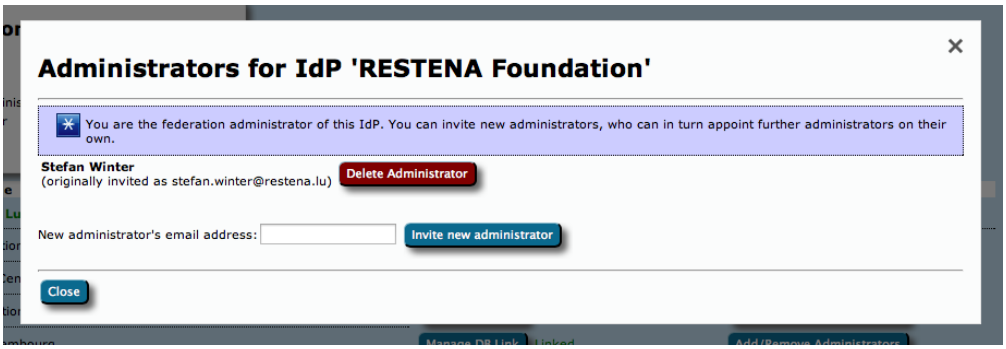
Once you have sent an invitation, you will be taken back to the federation management overview, which now lists the new pending invitation. You can revoke the invitation even before it expires after 24h if you feel the need to.



When an invitation has been redeemed, all federation administrators of your federation will receive an email notification by eduroam CAT confirming that a new IdP was created.

Add or delete representatives of existing IdPs

Once an IdP exists in CAT (i.e. once the first invitation token for the IdP has been redeemed by an invitee), the IdP admin can add more administrators or delete others as he sees fit. You can do the same though, by using the "Add/Remove Administrators" link on the right side of the list of IdPs. Please consult the guide to eduroam CAT for IdP administrators for further details of administrators management.



Take control over an IdP

In some exceptional circumstances, it may be necessary that you as the federation operator directly manipulate an IdP in your federation. By default, you do not get read or write access to IdP data of the IdPs which you have invited; they are expected to manage their own IdP in self-service.

Circumstances in which this is not sufficient may include, for example:

- an IdP admin has erroneously deleted himself and all other administrators of the IdP - so noone can manage them
- you are deprovisioning an IdP, but he refuses to delete his IdP in the eduroam CAT web interface
- the IdP admin requires assistance in setting up his IdP data, and you want to lend a hand

You can immediately add yourself as an IdP admin for each IdP in your federation by using the "Add/Remove Administrators" dialog box. For federation administrators, the dialog box has an additional button "Take control of this institution". By simply clicking this button, you will instantly become IdP administrator of this institution. Most notably, you do not need to send an email invitation to yourself; the process completes instantly.

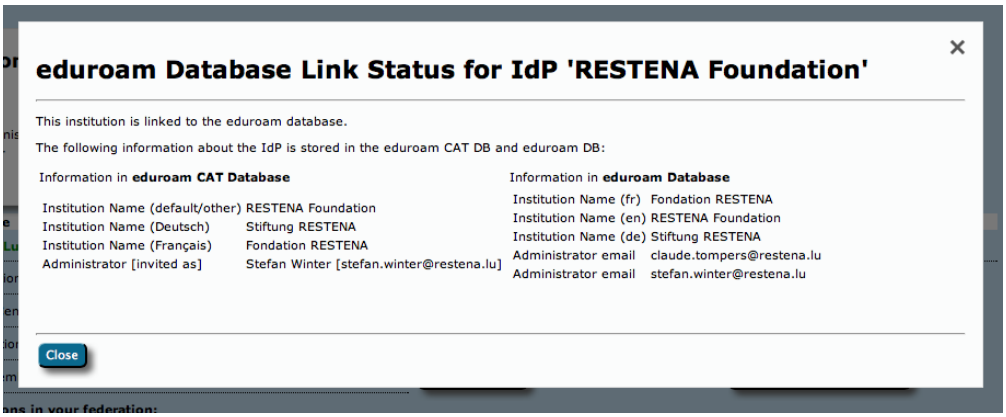
From this moment on, the IdP will be listed in your Profile Page, from where you can edit and can manipulate it as you see fit.

Manage the relationship between an IdP in eduroam CAT vs. an IdP in the official eduroam database

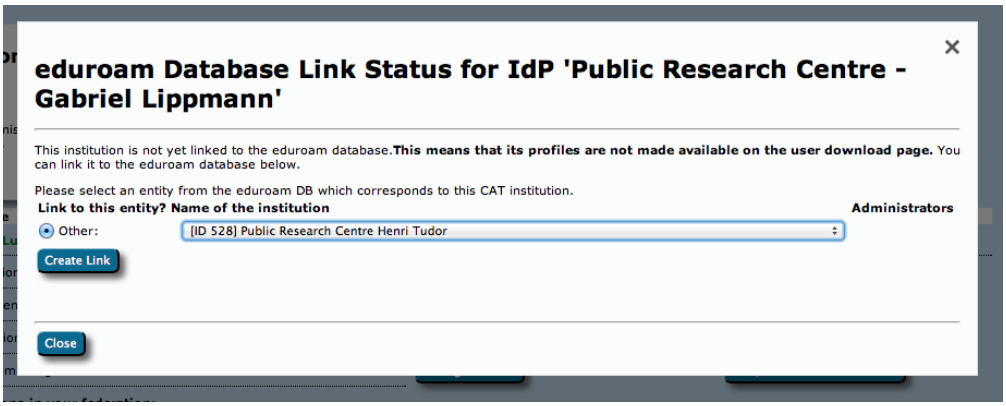
Since the official eduroa database contains only production-level eduroam IdPs, but the CAT can also be made available to IdPs which are still in a setup /bootstrap phase, the databases of the two tools are not in perfect sync. To avoid fragmentation and desynchronisation of the databases, federation administrators are encouraged to link the same IdP in both databases together.

In your federation overview page, you'll see the database link status on your dashboard page; the IdP is either "linked" or "NOT linked" to the eduroam database.

IdPs are automatically linked correctly if you used the "Existing IdP" dropdown list when inviting the first IdP administrator; then no further action is required. You can still click on the "Manage DB link" button to see some IdP details as seen from both databases.



If you created a new IdP instead, then this new IdP will not (ever) be linked automatically to an entity in the eduroam database. Once the IdP is in production and becomes listed in the eduroam database, you can add the link yourself by pushing the same "Manage DB link" button.



Simply select the appropriate entry from the dropdown list and click on "Create Link" to link the IdP as seen by eduroam CAT to the entity as seen by the eduroam database.

Once an IdP is linked, there is no user interface possibility to un-link them again, because there no use cases for this. Should the need to un-link an eduroam CAT IdP from an eduroam database entity, you should contact eduroam Operations by mail.

UI-less Automated Management: the Admin API (1.0.3)

As a federation administrator, depending on the number of IdPs in your federation, you may find it cumbersome to add institutions interactively. Or maybe you already have a customer self-service management system where authorised IdP admins could self-enroll without you being in the middle.

For cases like this, a small API was created which allows federation administrators to automate a limited amount of actions:

- Creation of a new IdP
- Checking the number of registered administrators of an IdP

Getting API access

The CAT Admin API requires the federation admin to be in possession of an API key. The API key is a long random string which needs to be used when executing API actions. The key is also bound to the federation; i.e. you can only create or query IdPs in your own federation with it.

API keys are distributed from eduroam Operation Team to federation admins on email request. Please contact eduroam Operations for your Admin API key.

API Basics

API actions are executed by sending an HTTP POST to https://cat.eduroam.org/admin/API.php. Different actions need different POST parameters as per the following table. More details about the actions is available in their respective sections below.

Action	Explanation	Required Parameters	Optional Parameters	Returns
NEWINST	Creates a new IdP in your federation	APIKEY NEWINST_PRIMARYADMIN	option, value (arrays of properties of the new institution)	**enrollment_URL**: The URL your new IdP admin must visit to be registered as IdP admin **inst_unique_id**: The unique identifier in CAT for the newly created institution
ADMINCOUNT	Queries the number of registered IdP admins	APIKEY INST_IDENTIFIER	none	**number_of_admins**: The total number of administrators of the institution
STATISTICS (in 1.0.4+)	Queries the number of downloads per device and in total	APIKEY	none	XML structure with intformation per-device with their admin & user downloads, and the grand total for all devices

The response is an XML file which either informs of success or failure.

Success responses may contain further details. All failure responses contain an integer error constant detailing what went wrong, along with a human-readable description:

Integer return value	Meaning	Explanation
1	ERROR_API_DISABLED	The Admin API is disabled on this instance of CAT.
2	ERROR_NO_APIKEY	The request did not contain an API Key.
3	ERROR_INVALID_APIKEY	The requst contained an API Key, but it was invalid.
4	ERROR_MISSING_PARAMETER	The selected action requires parameters, but at least one such parameter was missing.
5	ERROR_INVALID_PARAMETER	All required parameters for the action were specificed, but some are invalid.
6	ERROR_NO_ACTION	The request did not specify which action should be done.
7	ERROR_INVALID_ACTION	The request requested an action which is unknown to the system.

(defined in web/admin/API.php)

A typical error response looks like this:

```
<?xml>
<CAT-API-Response>
  <error>
    <code>3</code>
    <description>APIKEY is invalid</description>
  </error>
</CAT-API-Response>
```

Creating a new institution (Action: NEWINST)

This action creates a new institution in your federation. With only the required parameters, it is merely an empty shell of an institution. The API will return an enrollment URL, which you must communicate to your future IdP admin, and he must follow that link to bind his user identifier to the new institution.

The parameter NEWINST_PRIMARYADMIN is the value which will later be shown in the administrator management as "originally invited as". For user-interactive IdP creation, you are probably used to see email addresses in this field, because the invitations are then sent by email. Since the API puts the burden of showing the enrollment URL to your users on your shoulders, you are free to use any distribution channel for that (you could, for example, put the return code into an HTTP REDIRECT). Therefore, the text in this field is arbitrary. You can use it to correlate it to user IDs in your own customer management system or fill in arbitrary fantasy values. Just note that the values will be seen by the institution admin later on, so watch your wording 🙂

If you already know some properties of the institution (e.g. if you already register details about institutions in your own customer management system) then you can send almost all institution attributes inside the POST as optional parameters. The new institution will then be pre-provisioned with these attributes. The attribute-value format of the optional parameters is a bit peculiar:

The POST parameter option[Sx] specifies the name of the attribute to set; yes, that is a literal character "S" followed by an integer number of your choice (numbers do not need to be consecutive nor start at 1). All options can occur more than once.

Every POST parameter option[Sx] requires a corresponding value[Sx-<datatype>] parameter (see the table below for the data type identifiers).

Multi-language attributes also require a value[Sx-lang] parameter with the two-letter language code of the language this parameter is in (see the table below to see which attributes are multi-language). The language tag to use for "default/other languages" is "C".

The available options on the institution-wide level are:

Option Name	Explanation	value Data Type	Multi-language?
eap:ca_url	URL to a CA certificate which signs the server certificate (root or intermediary)	0	
eap:ca_file	file of a CA certificate which signs the server certificate (root or intermediary)	2	
eap:server_name	name (CN) of authorized RADIUS server	0	
general:geo_coordinates	geographical coordinates of the institution or a campus (a PHP-style serialised array of two numbers "lat" and "lon"), using a full stop "." as decimal separator	1	
general:instname	name of the institution	0	YES
general:logo_url	URL to a file containing institution logo	0	
general:logo_file	file containing institution logo	2	
general:SSID	additional SSID to configure, WPA2/AES only	0	
general:SSID_with_legacy	additional SSID to configure, WPA2/AES and WPA/TKIP	0	
support:email	email for users to contact for local instructions	0	YES
support:phone	telephone number for users to contact for local instructions	0	YES
support:url	URL where the user will find local instructions	0	YES

support:info_file	file containing the Terms of Use/Acceptable Use Policy for this IdP	2	YES

When only these options are set, the API will create a new institution without profiles. It is also possible to add a (one) profile to the institution automatically by including one or more of the following options (at least on the set of the first three must be set):

Option Name	Explanation	value Data Type	Multi-Langauge?
profile:name	The user-friendly name of this profile, in multiple languages	0	YES
profile: description	extra text to describe the profile to end-users	1	YES
profile: production	profile is ready and can be displayed on download page (only acceptable value is "on")	3	
profile-api: realm	the realm associated with this profile	0	
profile-api: anon	the local part of the anonymous outer identity to use, if that feature is turned on	0	
profile-api: useanon	turn on anonymous outer identity support	3	
profile-api: eaptype	integer value of a supported EAP type, as per the following table. Preference of EAP types is determined by the order induced by their option[Sx] sequence number. **value** / **EAP Type** 1 TTLS-PAP 2 PEAP-MSCHAPv2 3 TLS 4 FAST-GTC 5 TTLS-GTC 6 TTLS-MSCHAPv2 7 EAP-pwd	0	

Example

A new institution should be created:

- You have been given an API key "secretvalue" for your federation
- You want to create a new institution "A Random Institute" (this is the default name for all languages except French).
- The name in French should be "Institut de Chance".
- Their EAP server uses a root CA file which resides on your hard disk
- The institution logo is on your local hard disk as well
- Their support email address for all languages is "support@dev.null"
- The invitation handle for the primary institution admin should be "CUSTDB-135 John R. Doe"

For simplicity, you decide to simply use the command-line tool "curl" to craft a POST and register the institution. The command-line for curl reads:

```
curl \
-F APIKEY=secretvalue \
-F ACTION=NEWINST \
-F NEWINST_PRIMARYADMIN=CUSTDB-135%20John%20R.%20Doe \
-F option[S1]=general:instname \
-F value[S1-0]='A Random Institute!' \
-F value[S1-lang]=C \
-F option[S2]=general:instname \
-F value[S2-0]='Institut de Chance' \
-F value[S2-lang]=fr \
-F option[S3]=eap:ca_file \
-F value[S3-2]=@/home/swinter/scratch/someca.pem \
-F option[S4]=support:email \
-F value[S4-0]=support@dev.null \
-F value[S4-lang]=C \
-F option[S44]=general:logo_file \
-F value[S44-2]=@/home/swinter/balin/Pictures/GEANT2-logo.gif \
https://cat.eduroam.org/admin/API.php
```

The reply from the CAT API is then like:

```
<?xml>
<CAT-API-Response>
  <success action='NEWINST'>
    <enrollment_URL>https://cat.eduroam.org/admin/action_enrollment.php?
token=69bd8ea7e54e52f8aee887faeed7f5aca9657a983db121f5e865d46d931c4a75ce94cd2637cfc83b</enrollment_URL>
    <inst_unique_id>273</inst_unique_id>
  </success>
</CAT-API-Response>
```

You see that the URL to register is inside enrollment_URL; and you can take note that the institution was created in CAT with the unique identifier "273". You present that URL to your administrator, and ask him to click it and log into CAT to become admin of the IdP in question.

Later that day, you wonder if the admin has actually done that; you use the API action "ADMINCOUNT" for that.