Access to eduroam Operations Support Services

General

Access is granted by logging into the eduroam web authentication proxy (https://monitor.eduroam.org | Login) - the credentials used for this login are NOT eduroam credentials, but instead web SSO logins of academic AAI federations or, if such a federation does not exist for the user, social media providers.

User accounts are authorised for various eduroam Operations Support Services by adding appropriate privileges to the accounts on the eduroam web authentication proxy. This is done by eduroam Operations team sending a one-time token which, when redeemed, adds the privilege level to the user account.

Adding federation operator privilege level to a user account

The workflow for making a user account a recognised federation operator account are as follows; details for each step are given below:

- Ensure that name and email address of the user are listed in the official eduroam database
- Contact eduroam Operations, requesting the one-time token for adding the privilege
- Consume the one-time token by clicking on the corresponding link in the invitation mail and logging into the eduroam web authentication proxy

Listing user in the official eduroam database

The eduroam database is populated by parsing federation-provided metadata once every day. The data is expected on the main eduroam website of the federation, which is usually **www.eduroam.TLD** (where TLD is the country-code top-level domain of the federation); exceptions for the domain name exist.

The files to populate for federation administrator contact information are

```
http://www.eduroam.TLD/general/realm.xml
```

```
http://www.eduroam.TLD/general/ro.json
```

The contents of the XML and Json files are defined in the Schema and example XML/Json files exist at monitor.eduroam.org. New federations which provide their XML/Json file(s) for the first time should contact eduroam Operations so that their URL is added to the list of sources of information.

Contacting eduroam Operations

Federation operators in Europe should directly contact the GEANT mailing list of the eduroam Operations Team (eduroam-ot (at) lists.geant.org) and request their access to the eduroam Operations Support Services. Federation operators outside Europe should send their request to their representative of the Global eduroam Governance Committee (GeGC), who will in turn contact the eduroam Operations Team.

Consuming the one-time token

A user requesting access will be sent an email with detailed instructions on how to redeem the invitation token. It should be noted that the eduroam web authentication proxy requires a number of user attributes (predominantly the email address) to correlate the token with the user in question. If the AAI system in use does not reveal enough attributes, the account can still be given administrator privileges; but this then requires manual processing by eduroam OT and takes longer than the automatic self-service registration. Please consider revealing the AAI attributes for real name (displayName) and for email address (email), if possible.

Common authentication problems

The eduroam web authentication proxy allows for federated login - users are redirected to their Identity Provider, which authenticates the user and sends an assertion about the user back to the proxy.

This involves the protocol SAML and is an operation in which multiple administrative domains are touched. This leads to a number of breakpoints where the authentication process can fail. The most common such problems are listed below:

- No metadata found [IdP-side error, reported on IdP login page]
- Missing attributes for unique identifier [IdP-side error, reported on eduroam authentication proxy]
- Wrong attribute format for unique identifier [IdP-side error, reported on eduroam authentication proxy]