A guide to eduroam Managed IdP for IdP administrators

Terms of use

eduroam IdP administrators are bound by the requirements as set forth in the eduroam Service Definition. The specific service eduroam Managed IdP needs some additional terms on top of that baseline.

These terms and conditions are displayed and need to be acknowledged by eduroam Managed IdP administrator before they can start using the system (pop-up with sign-off requirement):

> 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 credentials that you issue can be linked by you to actual human end users of eduroam;
> - have to immediately revoke credentials of users when they leave or otherwise stop being a member of your institution;
> - will act upon notifications about possible network abuse by your end 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.
>
> With this product, eduroam Operations is not interested in and strives 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 eduroam access credentials 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.

eduroam end users are being presented a lightweight terms of use by the time they visit the download page for eduroam installers. Downloading the installer in question is deemed acceptance of those terms:

> You can now download a personalised eduroam® installation program.The installation program is strictly personal, to be used only on this device (device identifier, such as "Linux"), and it is not permitted to share this information with anyone.
>
> When the system detects abuse such as sharing login data with others, all access rights for you will be revoked and you may be sanctioned by your local eduroam® administrator.

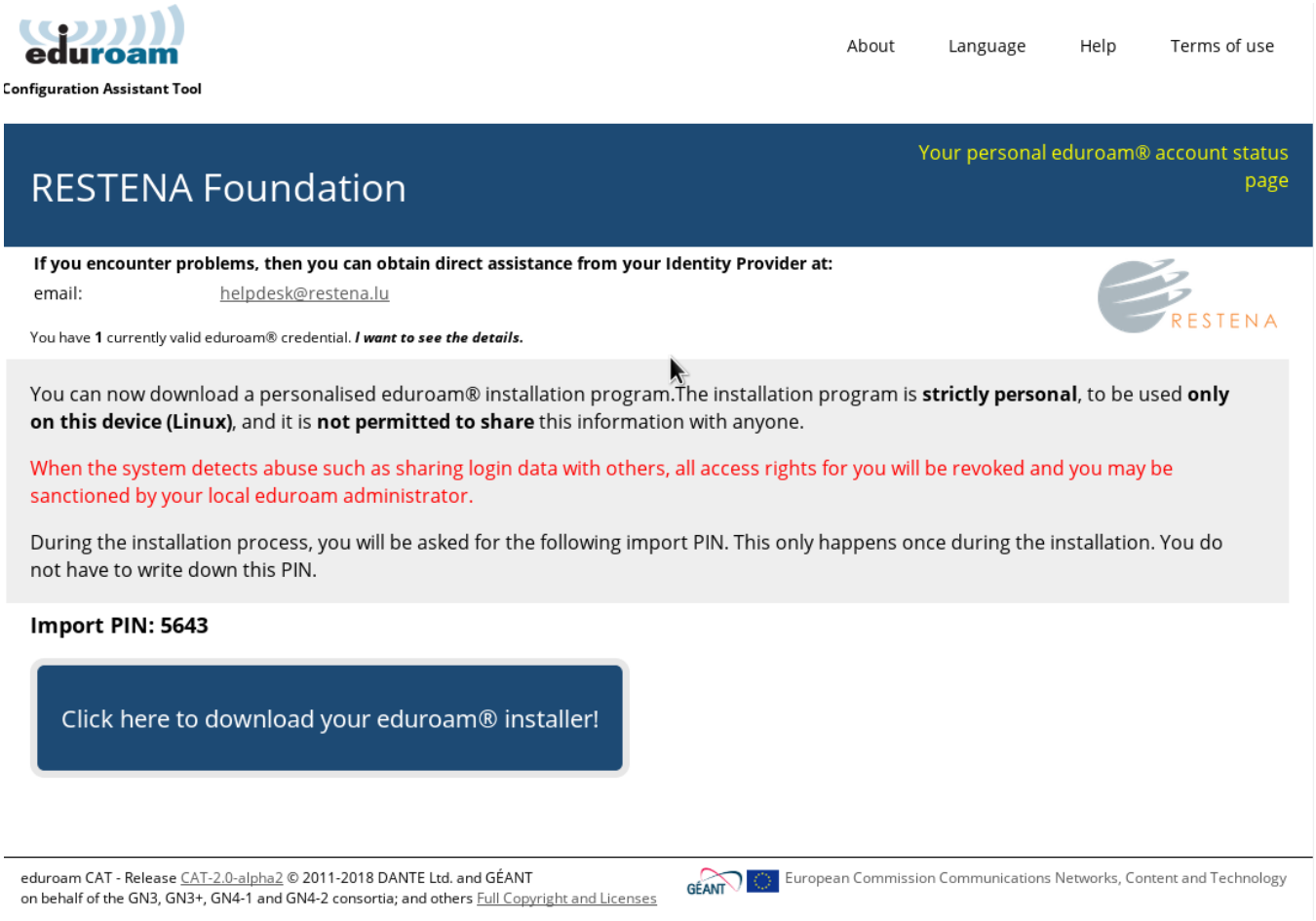
Purpose and scope

eduroam Managed IdP's purpose is to support you, an eduroam Identity Provider administrator, by allowing you to manage your eduroam end user base through a simple web interface, without a need for local technical infrastructure such as RADIUS servers or an identity management system.

eduroam Managed IdP takes your input regarding who your users are, and produces vouchers ("invitation tokens") which you can hand out to those users. They can then redeem those invitation tokens for a customised, personal eduroam installer for their computer or device. The customisation includes your IdP's name, location and logo, contact details for your helpdesk, and a user access credential in the form of a "client certificate" - don't worry if you do not know what that is. The installers can be produced in many languages; that way, you can even offer your users an installer in their native language!

Surprisingly many users do not have a clue which operating system they are using. eduroam Managed IdP thus auto-detects the operating system and automatically produces the matching installer.

Below is what your users will see when redeeming an invitation token:



Device Support

eduroam Managed IdP supports a broad selection of common end-user client devices. Unfortunately, if your users use a non-supported operating system, we are unable to provide the service to them. Please do let the authors know if a particular unsupported operating system is popular and we will investigate if it is possible to support it. Please contact us via the mailing list cat-users@lists.geant.org.

Notably, Android versions below 4.3 are not supported and likely never will be, sorry.

Support Policy for operating systems versions

eduroam CAT generally tries to follow vendors' end of life dates:

- Microsoft products:http://windows.microsoft.com/en-us/windows/lifecycle
  (next to go away: Windows Vista on April 11, 2017)
- Apple products: https://support.apple.com/en-gb/HT201624
  (next to go away, estimated: iPad - 1st gen (2016?), iPod touch - 3rd gen (2018?), iPhone - 4 (20XX?)

Scope

eduroam Managed IdP is not replacing your helpdesk! While we hope to do you a good service by taking the technical task of user account management and network admission checks into our hands, we can not take your users' phone calls or tell them how to fix problems on their computers. eduroam Managed IdP installers work on the supported platforms if these have not been modified beyond reason by the end-user, and we hope the installation process with them is intuitive enough; but we can not give you guarantees that you will not ever hear from failing users again.

Enrolling my institution for eduroam Managed IdP

Step 1: Requesting an entry for your IdP

eduroam Managed IdP follows the usual organisational model of eduroam: your eduroam National Roaming Operator (NRO) administrator has control over all the Identity Providers in his country or region. To manage your institution with eduroam Managed IdP, please let your NRO administrator know that you want to participate using your usual communications channels.

If the NRO administrator finds you eligible for the service, they will send you an invitation email with a token (the token is valid for 24 hours after sending it to you). You can then follow the supplied link with the token, log into the eduroam Managed IdP administration interface, and start managing your institution - see the next section for details of institution setup.

Step 2: Logging into eduroam Managed IdP

When clicking on the menu item "Manage eduroam admin access", you will be automatically sent to the eduroam Support Services' federated login service. This login service does not work with site-specific usernames and passwords; instead you are presented with a list of sources of identity. Choose any organization that you have an account with:

 * eduGAIN: many universities across Europe have already joined the educational Global Authorisation INfrastructure - if your organisation is among them, click on that institution and authenticate with your home organisation's usual web login credentials

 * Experimental: some institutions are in the process of joining eduGAIN, but are not production-level members; if that is the case for your institution, you might find your institution's authentication service in this Experimental list

 * Social Networks: if you cannot log in with your institution's credentials (for example, because your institution is not participating in eduGAIN), you can also log in using the federated login function of several popular social networks, including, but not limited to, Google and Facebook.

Some users have noted that none of the above options suits them: e.g. their institution is not participating in eduGAIN, and they have an aversion against using social networks. We understand that if a user finds all the numerous authentication options unacceptable, then he will have a hard time logging in. However, at this moment we do not have a good solution to that problem. It might be worth considering creating a social network account just for the purpose of logging in here; even if the service portfolio offered by e.g. Google is not interesting for the user, their authentication service in itself is useful on its own.

Configuring my IdP's properties

Overview

There are basically two groups of information which we need to ask of you before we can provide you with your eduroam Managed IdP profile:

- general information about your institution (e.g. logo, approximate location, name)

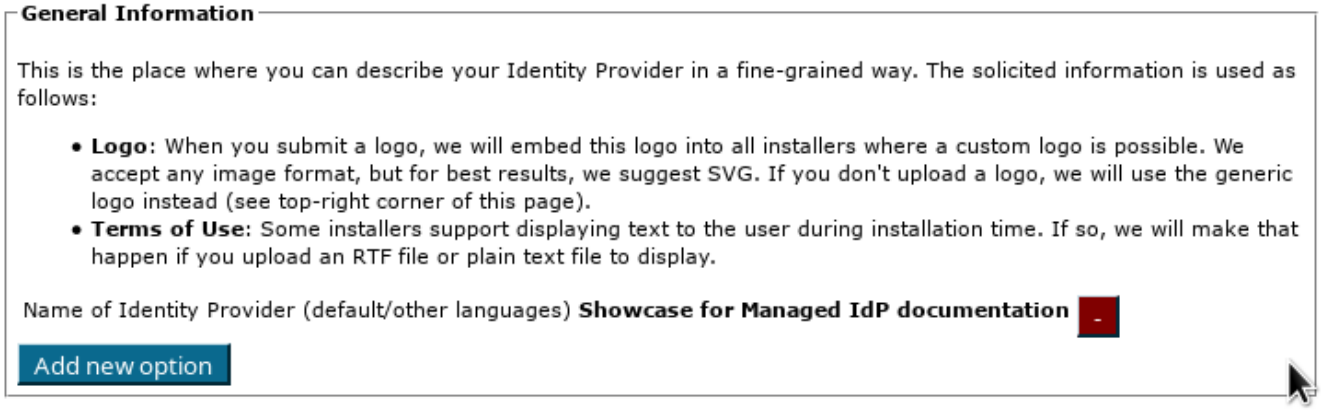
- helpdesk contact details (mail, phone, web)

To the largest extent possible, all the information is optional. If you choose not to let us know all the details we will still create installers, but they just won't contain as much information as they could. Please consider giving us as much information as possible. **At the very least, an email contact point for your end users is required so that they can reach out to you in case of questions.**
There are two governing principles regarding input and storage of information in the administrator user interface:

1. Textual information can be provided in many languages; one language representation should be set as the default language though - to have a string to present to users who want to use a language which wasn't explicitly configured.

Institution-wide Settings

After you've followed the invitation token from your national administrator, you'll be dropped right in the "Edit IdP" page. On that first time, you'll see a "wizard mode" which provides lots of explanatory text about the meaning of all the settings you can make. You can add and delete any of those options; don't be shy and try them all out! Adding a new option is done by pushing the corresponding button, selecting which option you want to set, and then the content of that new option. Changes will only be saved when you hit the "Continue ..." button on the bottom of the page.



When you re-visit the "Edit IdP" page later from the Institution Overview page, the explanatory texts are condensed in order not to overload the user interface. You'll certainly find your way around without the wizard texts.

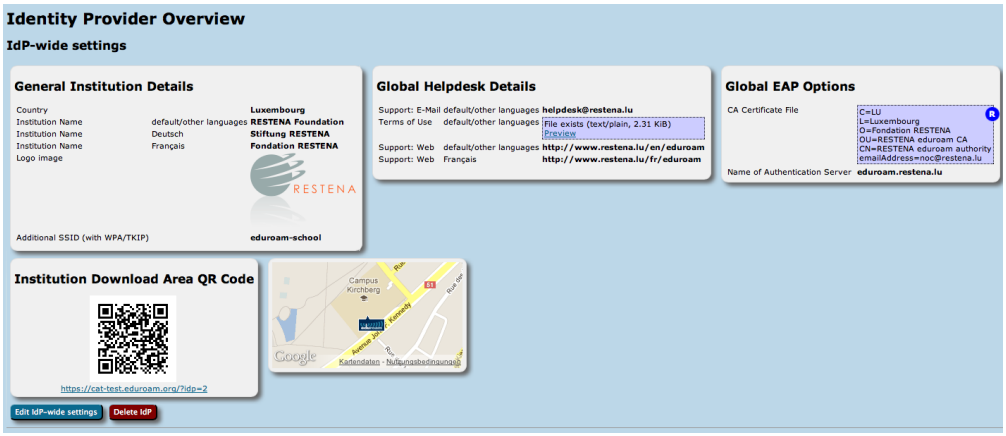
You can configure both the general information and the helpdesk details from this page.

General Information

Helpdesk Contact Details

Managing my users

On the institution dashboard page, you see the most important pieces of data that you have entered.



There is a button to create a new Managed IdP profile at the bottom. If you followed the wizard, it has already done that for you and you see an info card "Managed IdP" instead. It has a button labelled "Manage User Base".

The buttons take you to your user management page.

Installer visibility on the user download page

eduroam Managed IdP creates personal, private installers for just one user. The entry page of the eduroam Managed IdP website mostly serves as an entry point to administer your IdP; end users should not be directed to that entry page. They should be supplied with the links containing the individual invitation tokens instead, which take them directly to their personal overview page.

End User Personal Overview Page

Front Page

In case an end user erroneously visits the main entry page, the product maintains a list of all the IdPs which exist in the system. If the user finds and selects their institution in the list, the user is taken to a page hinting that they should contact their administrator for the personal link instead. There is no other functionality on the per-institution download page.

Other features

NRO Administrator API

A full access WEB API makes it possible to remote-control many aspects of the product. The corresponding documentation is maintained in the NRO documentation.

Getting Help with eduroam Managed IdP

If you have any questions about the eduroam Managed IdP website, please contact your eduroam National Roaming Operator first. They can escalate questions to the development team if need be. If you have questions about the underlying software, don't hesitate to ask on the mailing list cat-users@lists.geant.org . If possible, please subscribe to the list before posting; this guarantees that you'll get replies even if someone forgets a "reply to all", and also ensures that your post doesn't accidently get classified as spam and discarded.