

## Warning: Do not use web logins for eduroam

The eduroam Operations Team wishes to draw your attention to the fact that you should not use your eduroam credentials (i.e. username and password) to connect to the network via a login web page or “web redirect” system.

According to eduroam policy, a user gains access to the eduroam wireless network using an IEEE 802.1X client (so-called supplicant) installed on their computer. This client is pre-configured with user credentials so that users should be able to open their laptops and be immediately on-line. There is therefore no need to login via a web portal.

Please be aware that web portals are highly insecure for several reasons, such as:

- There is no way of telling if a web login page is genuine. Fake web login pages can be created easily by copying the look and layout of the original eduroam website, perhaps including the official logo.
- Usernames and passwords could be easily intercepted and used by unauthorised persons to “hijack” a user session or to access other personal information. This could occur if, for example, the same login and password is used for both email and university account management. In this case if a user's credentials are stolen, it's not just wireless connectivity that may be compromised.

If you come across a web page that asks you to login to a wireless network and it includes the eduroam name or logo, please be aware that this is in violation of the eduroam policy. In this case you are advised **not** to use the web page and instead to contact the relevant institution's helpdesk for assistance with connecting to eduroam.

Furthermore, please notify the eduroam Operations Team ([help@eduroam.org](mailto:help@eduroam.org)) about any web page that violates eduroam policy so that the Team can pursue the matter with the relevant institution.